Degreeproject

UNIVERSITY
OF SKÖVDE

A current state analysis of password policies for Swedish municipalities

Bachelor Degree Project in Informatics

First Cycle 30 credits

Autumn term 2024

Students: Filip Olsson and David Halén

Supervisor: Johan Zaxmy

Examiner: Thomas Fischer

Acknowledgements

We would like to express our sincerest thanks and apologies to our supervisor Johan Zaxmy for the insightful feedback, and for the inconvenience of having to act as a middle-man between us and the municipalities who wanted to verify the legitimacy of this study. Much nervosity has been quenched because of you. While our communication has been sparse during the duration of this project, we want to thank our examiner Thomas Fischer for his valuable feedback from the brief meeting we had and the reassurance that meeting instilled, and from the optional submission. The quality of this thesis project is all the better for it. A thank you also goes out to the municipalities that took their time to respond to our collection request. This thesis could not have been made without you. Special thanks to Daniel Ström for verifying the direct English translations of policy and law book extracts. Lastly, a heartfelt very special thanks to our friends Daniel Ström (again), Wilmer Nyman, Thea Ahlström Signal, and Anton Karlberg for much-needed respite during the weekends after a week of hard work.

Abstract

With cyber-attacks on the rise, secure authentication is an important commodity. With passwords being a prevalent authentication method, password creation policies need to be adapted to modern threats and social situations in order to assist users with upholding secure practices. This statement is as true in the public sector as it is in the private sector. This thesis aims to document the current state of password policies for municipalities in Sweden via the collection and analysis of password policies. The timing of this thesis is unfortunate, as the act of data collection, especially when it comes to a topic as sensitive as passwords, brings skepticism as a consequence of the current state of the world. Data collection requests were sent out to all 290 municipalities in Sweden, and 131 policy documents were ultimately obtained and analyzed. While the acquisition rate falls below the 166 that would have been needed for the scientific standard if data collection was from a random sample, it is believed that this amount still allows for a sufficiently detailed overview of the current landscape to be mapped out. The policies were subsequently anonymously coded using both an inductive and deductive approach. The analyzed data was used to measure the following: compliance with the policies compared to recommendations by five security agencies, how long a policy revision is used before a new revision is created and what changes between revisions, and whether a positive relation can be found between the creation date of a password policy and its specified minimum password length. The thesis found that 26% of the acquired policies currently in use were compliant with the recommendations by MSB, and 0.08% were compliant with ENISA. These rates might be a direct consequence of MSB having vague recommendations, and ENISA presenting what they deem is a strong password, not what they recommend as a minimum. Too few documents were acquired to make a general statement about policy age and changes between revisions. Furthermore, a significant positive relationship was found between password age and password length within the collected data.

Keywords: passwords, password creation, password policy, cyber-security, public sector, municipalities, Sweden, password recommendations

Contents

1 Introduction

As passwords are one of the most common authentication method, they are an attack vector and susceptible to compromises. With the NIS2-directive forcing essential organizations to adopt proactive cyber security measures, there is a need to evaluate existing systems and see if they need to be adapted to withstand modern threats.

According to the *National Institute of Standards and Technology* (NIST, Temoshok et al., 2022b), authentication to systems can be done in any combination of three ways:

- By something you know (A password or a PIN code)
- By something you have (A physical medium, such as an RFID tag)
- By something you are (Biometric data, such as a fingerprint)

Passwords are an authentication method based on what someone knows, and with passwords being very prevalent throughout society (Zimmermann and Gerber, 2020), there is a need to keep these secure and strong enough to avoid having them compromised.

This thesis intends to document the use of password policies within municipalities in Sweden in order to survey the policies' components and their adherence to recommendations, which can be of use in this task. As all documents that are created or stored within a Swedish public organization are part of the public domain, they may be retrieved if requested. This thesis has made such requests for documents and has compiled them into manageable statistics. It also intends to gauge how well municipalities adhere to recommendations published by organizations like MSB and ENISA.

While some studies has been made documenting the use of password policies, there has been no document that presents the composition and their usage for Swedish municipalities. The targeted audience of this report are the chief information officers working for Swedish municipalities. As such, a general understanding of IT is expected of those reading this thesis.

The evaluation of password strength is a well researched topic, but the evaluation of password policy strength is a lot less so. The calculation of password Entropy was a popular method used for user generated passwords to measure password strength in the past, with it being promoted by NIST, but has been shown to be insufficient in calculating actual strength. Since 2017, NIST has promoted the use of password length as a sole indicator. An interpretation of the recommendations by NIST, MSB, IIS, and ENISA has also been presented, as well as common user catalogs.

2 Background

In their threat intelligence report for 2024, the cyber security company Truesec claimed that cyberattacks were on the rise, with digital platforms being a prime target since they are an essential part of the operation of most organizations (Wåhlén et al., 2024). Cyberattacks can disrupt one or more of the three pillars of cyber security: confidentiality, availability, and integrity. A few common attacks, such as ransomware, can disrupt all of these pillars, while other attacks, such as business-compromised e-mails, can disrupt only a few. In the report, Truesec stated that the

most common attack vectors were phishing e-mails, vulnerability exploits, and stolen or brute-forced credentials to remote services, with vulnerabilities standing for 38% of all initial attack vectors in 2023, stolen or brute-forced credentials 26%, and phishing 23%. The primary action to guard against vulnerability exploits was keeping the systems up to date, having a robust filtering system, and educating personnel about phishing. For protection against brute-forced accounts, the primary protection was a robust password strategy.

The following chapter presents the key concepts that are used throughout the thesis. In addition, a brief overview of the vulnerabilities of passwords is presented, along with an evaluation of different methods used to evaluate the strength of user-created passwords. This is followed up by an overview of modern standards of password creation according to five different organizations. Furthermore, the background details the limitations of creating a password policy within five different AD environments. Finally, articles are presented that offer insight into the conclusions drawn within the area of password policy research.

2.1 The Vulnerabilities of Passwords

As passwords are an authentication method based on someone's knowledge of a string of text or code, they can be shared between individuals. As this knowledge can be shared, it can also be learned by unwanted parties. According to Keszthelyi (2013), passwords can be discovered in two ways: guessed or stolen. A password can be stolen in multiple ways. Passwords can be acquired via methods such as social manipulation, shoulder surfing, or breached databases. Guessing is yet another method. However, guessing usually involves factors such as probability and time, often combined with preparatory work, as passwords tend to contain personal information like date of birth or pet names or the knowledge of previous passwords. While social manipulation is an issue (Salahdine and Kaabouch, 2019), there is not much that strict password requirements can do to protect someone from sending their password to a malicious actor via e-mail. What strict password requirements can do, however, is to reduce the likelihood of them being compromised by a brute force attack. Keszthelyi (2013) states that storing passwords as plaintext in a database is a security risk. To avoid this security risk, the author states that most systems hashes passwords with a one-way hash, a method of creating a string of characters from a given input in such a way that the same input will always produce the given output, as well as making it impossible to know what the original input string was. Hashing seems to have historically been an effective mode of security as Denning (1982) states, "Because the stored passwords cannot be deciphered, they are completely safe even if the entire password file is (accidentally or maliciously) disclosed." As Moore's Law has suffered a slowdown as manufacturing techniques approach the physical barriers of what silicone can produce (IEEE IRDS, 2023), the computational power today is magnitudes greater than what was available in the 80s. Today, commercially available processors can do hash calculations fast enough to allow an actor to generate a large list of potential passwords, hash them, and compare the hashes to the hash of the password (Hendarto and Kurniawan, 2017). the Security Factory (2020) claims that an AWS p3.16xlarge instance – for the price of 25 USD per hour – can produce 632 gigahashes per second when trying to brute force the weak NTML-hash. With this computational power, all possible password combinations for six characters can be calculated and compared in a little over a second and under three hours for passwords with a character length of eight, assuming that the entire ASCII-table of printable characters is used. While the NTML-hash has been announced to be disabled in a future version of Windows 11, it still currently sees usage as a backup protocol for Kerberos (Palko, 2023). The *European Union Agency for Cyber security* (ENISA) state that with the use of public-domain tools, passwords as short as nine characters long can be brute forced in a matter of seconds. However, "any password that is not a common word, and is longer than 14 characters cannot be cracked with current computing means" (ENISA, 2022).

2.2 The Measurement of Password Policy Strength

This section presents two methods of comparing password policy strengths—password entropy and password length.

2.2.1 Entropy

Shannon (1948, as cited in Egelman et al., 2011) introduced the concept of information entropy as a means to measure unknown information due to random variables. The recommendations within NIST Electronic Authentication Guideline SP-800-63 have been the basis for many password policies since its publication, and one of the main takeaways is the measurement of password strength based on Shannon's information entropy (Egelman et al., 2011). Password entropy is defined as a measurement of the amount of uncertainty an attacker faces to determine the value of a secret, often counted in bits. The higher the bit-count, the less likely the password can be guessed. For randomly generated passwords, the calculation is x^y where x is the size of the character class and y is the length. This number is then rounded down to the closest bit (Burr et al., 2013). For example, if using only the numbers 0–9, the string has a character class of 10. In a randomly generated password with a length of six, using this 10-length character class, the calculation would be 10^6, which would equal $1,000,000$. This value is closest represented by $2^{33.3}$, which is rounded down to 33 bits.

For user-generated passwords, this calculation becomes much more complex as the passwords do not follow a random distribution. The characters that follow are usually arranged in such a way that they build words. Complexity refers to using multiple character classes, such as upper case letters and special characters. If capitalization is a requirement, these tend to be the first letter of the password, and if a special character is required, these tend to be the last (Burr et al., 2013). For this reason, the predictability of users' password creation habits results in some characters being "worth" less depending on what character it is and their position in a sequence. In summary, user-created passwords need to be longer in order to reach the same level of entropy that a randomly created password can achieve with fewer characters.

In NIST 800-63-2, a rough estimate of the entropy of user-created passwords was presented. The breakdown of the calculation is as follows: The first character is given an entropy value of four, with each additional character up to the length of eight adding another two. After that, each character adds an additional 1.5 bits up to the length of 20. Characters for position 21 and onwards are estimated to add only one additional bit. If the password adds a complexity requirement of a large character, and a non-alphabetic character—creating a three-character class password as NIST assumes lowercase is already used—a "bonus" of six bits of entropy is assigned to the bit-count of the password without any checks. In addition to length and dictionary requirements, additional entropy bits can be gained by using an extensive check to disallow the creation of passwords that can easily be broken with a dictionary attack, be it common words or common passwords. This type of check can give a variable "bonus" of entropy bits, ranging from zero to six, depending on password length and other factors. In NIST.SP.800-63-2 under appendix A, a table was provided over an estimated entropy of user-generated passwords in bits. An adaption of this table can be seen in Table 1.

	User Chosen				Randomly Chosen	
	94 Character Alphabet			10 char. alphabet	94 Character Alphabet	10 char. alphabet
Length Char.	No Checks	Dictionary Rule	Dict. & Composition Rule			
1	4	-	-	3	6.6	3.3
2	6	-	-	5	13.2	6.7
3	8	-	-	7	19.8	10.0
4	10	14	16	9	26.3	13.3
5	12	17	20	10	32.9	16.7
6	14	20	23	11	39.5	20.0
7	16	22	27	12	46.1	23.3
8	18	24	30	13	52.7	26.6
10	21	26	32	15	65.9	33.3
12	24	28	34	17	79.0	40.0
14	27	30	36	19	92.2	46.6
16	30	32	38	21	105.4	53.3
18	33	34	40	23	118.5	59.9
20	36	36	42	25	131.7	66.6
22	38	38	44	27	114.7	73.3
24	40	40	46	29	158.0	79.9
30	46	46	52	35	197.2	99.9
40	56	56	62	45	263.4	133.2

Table 1: A table that shows the estimated character length to bits of entropy. Note: Adapted from "Electronic Authentication Guideline" table A.1 by W. Burr et al., 2013, NIST Special Publication (SP) 800-63-2. No copyright.

2.2.2 Addressing the Reliability of Entropy

By analyzing the RockYou32 list, Weir et al. (2010) discovered that the usage of digits, special characters, and capital letters was neither uniformly distributed nor evenly used. Out of all of the passwords that had numbers in them, the single digit "1" was used the most with a 10.98% usage rate, with the single digit "2" and number combination "123" being used the second and third most with a usage rate of 2.79% and 2.29% respectively. The authors also discovered that for passwords seven characters or longer that contained both characters and digits, the numbers were appended 77.46% of the time. When examining RockYou_training28−32 and including only passwords containing uppercase characters with a length of seven, 53.56% of all the passwords only contained capital letters, with 35.69% of them starting with a capital letter and continuing with lowercase ones. If both lowercase and uppercase characters were required, this would increase the second option to 76.85%. On the usage of special characters, "." had a frequency of 17.81%, with "_" and "!" being in second and third place with a usage of 14.72% and 11.34%, respectively. The character "@" was on rank six and had a usage rate of 7.19%.

This contrasts with the findings by Komanduri et al. (2011) in which they surveyed 5,000 people to create passwords. For people creating at least eight-character-long passwords that required a number, a special character, and a capital letter, the occurrence of "@" was at first place with 22.78%, with "!" and "$" being in the second and third place with 21.71% and 10.46% respectively. ".", which was used the most in the study written by Weir et al., saw a usage rate of 6.04% at sixth place.

While both of the studies do provide different usage rates for different characters, it is clear that the distribution follows a pattern. Since the release of NIST 800-63-2 in 2013, the guidelines have been updated with a third revision in 2017 (P. A. Grassi et al., 2017), with a fourth waiting to be approved for release by the time of writing (Temoshok et al., 2022a). In part B of the third revision, it is acknowledged that despite entropy being an oft-used method to determine password entropy, it is in no way an accurate way to calculate the strength of user-created passwords (P. Grassi et al., 2017).

2.2.3 Password Length

Research suggests that password length is the leading factor that makes a password both strong and user-friendly (Kelley et al., 2012; Komanduri et al., 2011; Proctor et al., 2002; Shay et al., 2016). Long passwords without any complexity requirements are suggested to not only be harder to compromise in a brute force attack, but also more convenient for the end-users to both create and remember (Komanduri et al., 2011). However, having no requirements other than minimum length may entice some users to create absurdly simple and easily guessable passwords, such as "passwordpassword" or "abcdefgh12345678" (Shay et al., 2016). This suggests that the inclusion of some complexity requirements is, for the most part, a means to hinder users from acting predictably, while the length is what contributes to strong and convenient passwords. Tan et al. (2020) suggest that the use of password complexity should be phased out and that length requirements combined with a blocklist or a password strength check provide better security and memorability.

2.2.4 Comparing the Different Methods

While entropy is a solid measurement of strength in randomly generated passwords, it has been shown to be unreliable for user-generated passwords. Its unreliability in determining the password strength might not be a hindrance if the relative strength between two user-generated passwords could still be accurately represented by their difference in calculated entropy, but as no sources were found that break down the complexity requirement into its entropy-contributing components, nor any that support the relative strength between two entropy values, the usage of entropy as a measurement of password policy strength within this thesis was rejected.

2.3 Modern Recommendations

Password policies exist to create a minimum level of password strength by restricting users' ability to create weak passwords. There are several organizations like ENISA that exist to help organizations and private individuals alike improve their information security by publishing recommendations regarding secure practices for activities ranging from browsing the web to secure workplace conduct. The password recommendations from five different organizations is detailed in the following subsections.

2.3.1 NIST's Recommendations

In the NIST Digital Identity Guidelines SP 800-63-3, released in 2017, the organization provides a list of three levels of authentication assurance (P. A. Grassi et al., 2017). At level 1, there is "some assurance" that the claimant is who they state they are. At level 2, this can be done with a high level of confidence by having two distinct authenticator-factors identifying the user. Level 3 provided a very high confidence level and requires that at least one of these authenticator methods be bound to a physical device. In this revision of the SP 800-63 document, their guidelines stated that "Memorized secrets [passwords] SHALL be at least eight characters in length" for an Authenticator Assurance Level of 1, which only provided some assurance of authentication, a statement that was not present in the second revision released in August 2013 (Burr et al., 2013; P. Grassi et al., 2017). Based on this, a conclusion can be drawn that after 2017, NIST has not been holding any confidence for passwords shorter than eight characters in length, which was something that was not explicitly stated before. NIST moved away from

the notion that complexity would be a favorable factor toward user-created passwords that are harder to compromise with a brute force attack. This was due to more modern research, which came to the conclusion that users have a tendency to respond in predictably when faced with composition-rule requirements (P. Grassi et al., 2017). Rather, the author states that long passwords simply provide more security whilst working in tandem with limiting the rate of login attempts. Furthermore, NIST currently recommends against forcing users to regularly update their passwords due to users having the tendency to choose weak passwords if they know that they will have to create a new one in the near future. Rather, password changes should instead be enforced in the event of an attack (NIST, 2022). See Table 2 for a summarization of the recommendations.

2.3.2 MSB's Recommendations

The *Swedish Civil Contingencies Agency* (MSB, Myndigheten för samhällsskydd och beredskap), is an administrative authority under the Swedish government. They are responsible for providing information regarding actions taken before, during, and after accidents, crises, and even war (MSB, 2024b). MSB provides recommendations for private citizens regarding how they can secure their passwords. It is worth noting that MSB only provides general tips rather than recommendations based on a concrete standard. No concrete recommendation for minimum password length is provided. However, MSB (2024a) provide several factors that constitute a strong password:

- Use of passphrases
- No Swedish characters
- No common words
- No words or names that can be connected to you as an individual

The use of passphrases helps attain a password that is both sufficiently long and memorable, and introducing a mix of upper- and lowercase letters can achieve additional complexity. Swedish characters can turn out to be a hindrance for the user in the event that they are forced to use a non-Swedish keyboard. As such, the use of Swedish characters has nothing to do with the actual strength, as it rather is a safety precaution for convenience's sake. Common words and words that have a personal tie to the user lead to a higher risk of guessability in the password, and MSB recommends that the user should consider avoiding them. Additional tips include the use of:

- Password managers
- Multi-factor authorization
- Unique passwords
- Stronger passwords for important services

See Table 2 for a summarization of the recommendations.

2.3.3 IIS's Recommendations

The *Swedish Internet Foundation* (Internetstiftelsen i Sverige, IIS, Löwinder, 2016) has published recommendations for password creation and management in which they state that passwords shorter than 10 characters are generally considered weak. The recommendations state that it is not good practice to change a password if it has not been compromised and that it offers no security benefit as stolen passwords are often promptly used, and that forced, time-based password changes on short intervals reduce users' perception of the password's value, and will thus be more prone to be shared with others (Löwinder, 2016, p. 43). This practice has been used for a long time and has been hard to kill off, according to IIS. For users with many passwords to remember, it is recommended that they consider using several levels of passwords. The user should consider which accounts are the most sensitive and focus on assigning strong passwords to those accounts, while passwords linked to less important accounts may be less secure and even reused if the user deems it appropriate. The IIS suggests that the more complex a password is, the better. If a user does not want to implement a complex password, they suggest the usage of password phrases as these tend to be longer and easier to remember than traditional passwords, but state as some complexity is removed, the length of the password is a bigger contribution factor to password strength. The IIS states that while password generators are a great source for strong and truly random passwords, they are not recommended for use in a corporate setting. This is motivated by their statement that the creator of the tool can not be fully trusted. In addition to the general recommendations for password creation and management, the report also lists six tips for system administrators and owners.

- Always change preset passwords for administration and remote management accounts.
- Log past login attempts and show these to the user so they can report if a login attempt has happened that they were not responsible for.
- If passwords are user-defined, educate users in good password creation and blocklist commonly used passwords.
- Never store passwords in plaintext and disallow users to save passwords in web browsers.
- Generate passwords, but let the users choose and influence the password selection and lock accounts after a number of failed attempts.
- Administrator accounts and accounts for remote management should have more strict password requirements.

The report states that passwords must never be written down digitally in plaintext, but that writing them down on paper is fine as long as they are handled with care by the user. Additionally, the items in the following list are considered as causes of especially poor passwords:

- Personal information (ex. name of pet)
- Sequences (ex. 12345)
- Words found in a lexicon

See Table 2 for a summarization of the recommendations.

2.3.4 SUNET's Requirements

The *Swedish University Computer Network* (SUNET) is the organization that provides data communication for universities and public organizations with ties to higher education or research (SUNET, n.d.). While providing no recommendations for other organizations inside or outside of the education sector, they do host an infrastructure for authentication to services like SAML WebSSO and eduroam, SWAMID, and provide rules for authentication for these services. SWAMID has three levels of identity assurance. With an identity assurance level of 1, SUNET states that it is very likely that the account belongs to and is used by a human, not a robot or a piece of software. The information associated with an account of this level is usually self-asserted and holds the user responsible for the account's security (SUNET, 2020a). With an identity assurance level of 2, SUNET states that this level can more positively identify the user, tying the account to a physical person. The information associated with an account of this level should be an account the organization is responsible for (SUNET, 2020b). With an identity assurance level of 3, SUNET states that this level can even more positively identify a user, verifying the identity of the person logging in. At this level, multi-factor login is mandatory (SUNET, 2020c). The differences in requirements between these levels are mostly due to how these accounts are managed, and all levels require a password of at least 24 bits of entropy, as defined in NIST SP 800-63-2, released in 2013. For a randomly generated password using the ASCII character set, the password has to be of four characters to satisfy the 24-bit requirement, or eight characters if only numbers, see Table 1. Without any restrictions and assuming that only lowercase characters are used, a 24-bit entropy can be achieved by a character length of 12. As stated under 2.2.1, if a capital letter, lowercase letter, and a numeric or special character are used six additional bits, Burr et al. (2013) states that the password is estimated to have six additional bits in addition to the length. A password with 24 bits of entropy using these three character classes would, therefore, require a character length of eight. Providing recommendations for municipalities is outside the scope of SUNET, and it is acknowledged that the requirements presented are not intended to be used as recommendations. Nevertheless, SUNET is still included in this study out of curiosity due to its inclusion of entropy as a password strength indicator, as well as out of interest in seeing the requirements of one sector compared with another. See Table 2 for a summarization of the requirements.

2.3.5 ENISA's Recommendations

ENISA is an agency within the European Union with the goal of achieving higher cyber security standards across Europe (ENISA, 2024). In 2021, ENISA published a leaflet containing steps to secure a small to medium-sized enterprise. In this leaflet, they recommend creating passwords made out of three common random words, using both uppercase and lowercase characters. Numbers and special characters are referred to as an optional add-on. Furthermore, it is recommended to avoid the obvious in the shape of commonly used dictionary words such as "password", predictable sequences like "abc123", and personal info that can be derived from the user. In addition to this, ENISA recommend that passwords are not to be shared with employees or reused elsewhere and recommend the usage of multi-factor authentication and dedicated password managers (ENISA, 2021). Assuming that English dictionary words are used, this would create a password that would be slightly longer than 15 on average (Lindner, 2024). This assumption seems to follow the statement made by ENISA (2022) about password longer than 14 being considered secure, which was presented in section 2.1. See Table 2 for a summarization of the recommendations.

Recommendation	NIST	MSB	IIS	SUNET	ENISA
Minimum length	8	Encouraged	10	–	15
Complexity	Discouraged	Encouraged	Encouraged	–	2
Forced change	Discouraged	–	Discouraged	–	–
No Unicode	–	Encouraged	–	–	–
No personal info	–	Yes	–	–	Yes
No sequences	–	–	Yes	–	Yes
Blocklist	–	Yes	Yes	–	Yes
MFA	Encouraged	Encouraged	–	–	Encouraged
Write down	–	–	Safe	–	–
Entropy	–	–	–	24 bits	–

Table 2: A table showing the summarizing of the published recommendations and requirements.

Setting	Minimum value	Maximum value
Password History	0	24
Maximum password age	0	999
Minimum password age	0	998
Minimum password length	0	14

Table 3: Windows AD password policy settings and valid values

2.4 System Limitations

Different IT solutions may have different limitations in place for what is configurable within a password policy. These may restrict the design of a password policy and thus need to be considered. As of February 2023, Microsoft holds about 70% of the desktop, tablet, and console OS market share. This suggests that Windows stands for a large part of the user-facing interactions within IT (Sherif, 2024). While it is assumed that many Swedish municipalities utilize Microsoft's software for their IT solutions, other alternatives like Citrix Workplaces or Google Workspaces exist and could be deployed.

2.4.1 Windows AD

In Windows AD, only a few customization options are available to an administrator when it comes to password policies. Microsoft details which settings can be configured on their website (Pamnani, 2017). Values can be set for several settings in which zero means that the criteria is not enforced by the policy. Password history can be configured to store a user's previously used passwords. If a newly created password matches any of the stored passwords in the user's history, they will be prompted to select a new one. Maximum password age correlates to a value in days for which a password is valid. Once the time is up, a new password has to be created. Minimum password days correlates to a value in days that has to transpire before the user can create a new password. Minimum password length is the minimum number of characters that a user-created password has to contain. The minimum and maximum values that can be configured can be seen in Table 3.

Of note is the minimum password length being limited to a maximum value of 14 characters by default. While this is a high value considering that none of the organizations in 2.2 recommend

a password longer than this, and since Pamnani (2017) writes that Microsoft themselves recommend a minimum of eight characters, it seems like a hindrance in case an admin wants to enforce a minimum length of 15 or higher. An update to Windows 10 released in 2020 allows for the configuring of a 15 or more characters minimum password policy, but this option is not enabled by default as it may break backward compatibility with older systems (Microsoft, 2021). Windows also has an AD setting that checks if a password meets certain complexity criteria. In order for a password to pass the check, it has to contain at least one character from three out of five categories. The categories are as follows:

- Uppercase European letters (A-Z with and without diacritic marks, Á, Ñ, etc), which includes Greek and Cyrillic characters
- Lowercase European letters (a-z, with and without diacritic marks, sharp-s "ß"), includes Greek and Cyrillic characters
- Base 10 digits (0-9)
- Special characters (’-!"#$%&()*,./:;?@[]^_‘{}|~+<=>), £ and € are not included
- Non-uppercase or lowercase Unicode characters that are categorized as alphabetic letters. Includes Unicode characters from Asian languages

There is no setting to configure the amount of categories that have to be included in a password. The only options are to forcibly include three mandatory categories or none at all.

2.4.2 Microsoft Entra ID

The password policy settings differ slightly between a locally run Windows AD and Microsoft Entra ID. This policy is mostly unable to be configured, and the only settings that can be changed are when and if passwords can expire, as well as a custom list of banned passwords and parameters for account lockout (Hall et al., 2024). The article by Hall et al. (2024) details the preconfigured password policy for cloud-only users:

- A minimum of eight and a maximum of 256 characters
- At least one character from three of the four following groups:
  - Lowercase characters
  - Uppercase characters
  - Base 10 digits (0-9)
  - Symbols (’-!"#$%&()*,./:;?@[]^_‘{}|~+<=>)

Note the lack of the fifth character class seen in the list in section 2.4.1. In addition, Unicode characters are not allowed. This policy almost completely matches the requirements set within Windows AD. Unlike what is possible in Windows AD, an admin may not configure a higher value for the minimum number of characters, yet it is similarly restricted to a set number of character groups that need to be present even though the number of character groups is lower. Users can not use their last password after changing their password, but their last password can be used again after resetting a forgotten password.

2.4.3 Okta

Okta is an identity platform used as an interface for authentication for applications and services (Okta, n.d.-a). While Okta itself can be used as an intermediate layer between an application and a user directory like AD or LDAP, it also can feature its own user catalog. The company states that if an AD or LDAP backend is used, the password policies set in Okta must be compliant with the password requirements set within the individual catalogs as well (Okta, n.d.-c). Within Okta, it is possible to set a minimum length of four and a maximum of 30 characters, with eight being the default for Okta's user catalog. For instances that use AD or LDAP as a backend, the respective limitations for minimum password lengths for those systems are used. For complexity requirements, Okta states the possibility to "Select options to define the level of complexity that is required for user passwords" but provides no examples or information about what these options might be (Okta, n.d.-b).

2.4.4 Citrix Workspaces

While Citrix Workspaces is a platform of tools on its own, it features no user catalog but can be configured to use either Windows AD or Okta as a backend. While it is possible to write password policies within Citrix Workspaces, these exist only to be presented to the user when conducting a password change within the platform. The rules are not evaluated and are meant to reflect the requirements of the backend (Citrix, 2024).

2.4.5 Google Workspaces

Google Workspaces is a set of cloud-based collaboration apps that Google provides. While normally free to use, additional administration features can be purchased, which allows an administrator to configure rights for a group of users, among other things. Certain password requirements can be enforced by an admin, but it is not entirely clear what is enforced in actuality. What is explicitly defined is the password length, which may be between eight and 100 characters (Google, n.d.-b). Admins have the option to enforce strong password checks, but what this entails is not entirely transparent. Other than general recommendations, Google (n.d.-a) states that a strong password can not be "particularly weak". "Password123" is a provided example of a weak password, which may suggest the use of a blocklist or some other composition check. Further, the password must not have been used before. However, admins can enable the option to let users reuse previously used passwords if they so choose. Additionally, it is stated that a password can not start or end with a blank space, and accents or accented characters can not be used. Furthermore, admins can configure user passwords to expire after a set amount of time. However, the amount of days that an admin is able to configure before passwords expire is not specified by Google. This is the most restrictive AD alternative out of the ones presented due to its non-transparent nature and checkbox-based admin options.

2.5 Previous Research

Gerlitz et al. (2021) performed a survey to study German companies' adherence to password recommendations presented by organizations like NIST and the German *Federal Office for Information Security* (BSI, Bundesamt für Sicherheit in der Informationstechnik). The survey was answered by 83 people, and out of these, 68 used a central authentication system. The following metrics were analyzed: the minimum password length, password complexity requirements, the

maximum password age and the password history length, the allowed character sets, and the use of blocklists. They concluded that 95% of the people surveyed specified a length requirement, and out of these 52%, a minimum character length of eight. For password complexity, 89% of the companies had specified a requirement, with 50% requiring three out of four classes and 27% requiring all four. 7% of the companies did not specify a complexity requirement. For password age, 34% used a maximum age of 90 days, with 180 being used by 14% and 365 days being used by 11%. Only 3% of the companies explicitly stated that they did not retire passwords based on age. 41% of the companies stated that they checked passwords against common or leaked passwords. The authors interpret the NIST guidelines as a character length of at least eight and no complexity requirement from the newer NIST documents, but "sufficient" complexity was recommended by the older revisions. From the surveys, the authors concluded that 89% of the companies followed the requirements of length, with 52% being at the minimum of eight. The authors also state that the NIST advises against setting a maximum password age. As mentioned before, only 3% of the companies follow this recommendation. BSI's old documented recommendations had no concrete definitions of their recommendations. BSI defined their recommended minimum password length as "sufficient", along with a "sufficient" level of complexity and an "appropriate" maximum password length. BSI's new recommendations introduced an element called quality, which their entire recommendations were based upon. The level of quality was required to be "appropriate". Since the recommendations were not concretely defined and were solely based on ambiguous terms, measurement of compliance towards BSI was not possible.

A study by Gerlitz et al. (2023) had the aim to see if the password policies for German companies had been updated to follow the BSI's new recommendations, which were published in 2020. The greatest change, according to the authors, was the omission of a recommendation to use password expiry. The authors conducted three surveys on the companies' password requirements: one survey eight months after the change, another two years after the change, and the last three years after the change. They were then compared to data gathered in 2019. The study claims that within the surveyed companies, the usage of two-factor authentication rose by 20 percentage points and that longer passwords, consisting of 12 characters and up, were more common in 2023 than in 2019. The study also claims that while over 40% of the participants claimed that they still use password expiry in 2023, this is statistically significantly less than in 2019.

Norris et al. (2021) conducted a survey of American local governments to explore their cyber security practices, such as location of responsibility within cyber security, outsourcing, cyber security insurance, change of budgets in the last five years, use of cyber security tools, adoptions of practices and actions taken, as well as awareness and support of cyber security of the local officials. The survey received a response rate of 11.9%, with 406 counties and municipalities responding out of 3,423. The study categorized the local governments based on population size, geographical division, and form of government. A cross-tabulation analysis was done, and the correlation coefficient between local government characteristics and the cyber security answers was calculated. Norris et al. stated that associations between local government characteristics and IT as been established in literature before (Norris, 1984, 2010; Norris & Campillo, 2002; Norris & Kraemer, 1996; Norris & Moon, 2005; Norris & Reddick, 2013; Reddick & Norris, 2013 as cited in Norris et al., 2021). Based on the data gathered from the survey, the authors concluded that there was no robust pattern of recent investments. For cyber security policy adoptions, the authors concluded that 70.7% of the local governments did have password creation rules, 70.0% did require periodic password changes, and 40.1% did use a cyber security policy, standard, strategy, or plan. When asked to rate the effectiveness of these policies, 12.0% stated that their password creation rules have a very low or low effectiveness, 31.7% stated that the effectiveness was average, and 56.3% stated that it was high or very high. On the topic of

periodic password change requirements, 11.3% stated that the effectiveness was either very low or low, 30.4% stated that it was average, while 58.3% stated that it was high or very high. For cyber security policies, 29.9% stated that the effectiveness was very low or low, 50.5% that it was average, and 19.6% that it was high or very high. The authors did not state if effectiveness is a measurement of the enforcement of the policy or if it is the policy's positive impact on the local government's cyber security. When asked to rate their policies, 31.3% stated that they followed best practices, 32.2% stated that they were one generation behind, 26.3% stated that they were more than one generation behind, and 10.3% stated that they did not know. Norris et al. wrote that the previously stated low effectiveness might be a result of not following best practices. When examining cross-tabulations, only 16.2% of the variable pair did produce a significance of $P =< 0.05$ (5% chance the differences were due to standard deviation), but the authors concluded that the relationships did not follow the expected pattern, and while measuring the relationship with Cramér's V statistic, they found that the relationships were generally weak with a coefficient between 0.20 and 0.29.

Hatcher et al. (2020) aimed to find out if municipalities in the United States had proper cyber security policies implemented. This was done by sending out surveys to public officials via e-mail, which contained questions regarding how the cities were planning around cyber security, the resources needed to conduct those plans, and how policies were implemented. The authors had a response rate of a mere 7% out of the 2,436 e-mails sent to municipalities. They argued that this was due to the low response rate of surveys, especially ones regarding cyber security, which is considered a sensitive subject. However, they argued that the data collected was still rich. 71% of the respondents had a formal cyber security policy in place, while 77% of the municipalities without one were planning to have one implemented. It was found that larger cities were more likely to have cyber security policies in place, most likely attributed to larger cities having a higher budget. Perhaps unsurprisingly, municipalities with a defined formal cyber-security policy tended to show signs of better cyber-security practices. The authors concluded that American municipalities must maintain details regarding cyber security attacks, hire professionals to help create more effective IT policies, try to get more funding, and lastly, make cyber security a management function by providing training for officials.

An article by Sparrius et al. (2021) had the aim to analyze UK schools' *Information security policies* (ISP) that were directed to school employees. The main purpose of this study was to analyze the content of the ISPs and list what was there and what was missing. In addition to this, the schools' ISPs that were analyzed were looked at one year after the first gathering to see if they had been updated. Out of the 100 ISPs analyzed, 72 policies were due for an update in the coming year. Out of these 72 policies that were overdue, when examined a year later, 31 had no changes made, and 24 of them only had superficial changes to the ISPs, in which a date or a name was changed.

3 Problem Formulation

The following section highlights the study's aims and research questions. A motivation that explains why the authors claim the thesis to be an important contribution to the research area is provided, along with how this thesis differs from the previous research presented in section 2.5. A description of identified delimitations is presented, which defines the scopes and boundaries of this thesis.

3.1 Study Aims

This study aims to provide insight into the current state of password security for municipalities in Sweden and document the frequency of the changes to those policies regarding passwords. This study also intends to gauge how closely these policies adhere to recommendations published by information security organizations. Furthermore, it tries to gauge whether more recently created or revised password policies adopt higher password length standards, as password policy strength is hard to quantify, see section 2.2.3.

RQ 1: What are the password requirements of the municipalities, and how do those requirements adhere to the recommendations provided by security agencies such as NIST?
RQ 2: How long have the municipalities been using their current password policy, and how long did they use their previous one? What changes occurred between the last revision and the current policy?
RQ 3: Do newer password policies require longer passwords, and what is the relationship between a policy's revision or effective date and their required minimum length?

3.2 Motivation

Due to the lack of a singular document detailing current practices regarding password policies for municipalities, this paper is motivated to provide an overview of the current password policy landscape. Furthermore, understanding the current practices in use could shed light upon any vulnerabilities or insecure practices, if any are found. Similarly to a study by Gerlitz et al. (2021), this thesis aims to track the compliance to recommendations. However, unlike the study by Gerlitz et al., this thesis also aims to document the current state of password practices. This thesis also differs in that it looks at Swedish municipalities while their study looks at German companies. This thesis shares similarities with Norris et al. (2021) as both inspect municipalities and policies in place; what variables are looked at, the data collection method, and the country of study differ, however. Hatcher et al. (2020) studied if American municipalities have proper cyber security policies implemented as well as the process of implementing said policies. This study is driven partly by the same motivation but with Swedish municipalities as a focus. This thesis similarly wants to provide an overview of cyber security policies being implemented by municipalities. Unlike the mentioned article, it also intends to find where the basis of said policies stems from and is less interested in the detailed process behind creating the policies. Further, this thesis implements a different data collection method. The paper from Sparrius et al. (2021) differs in terms of aim. While that article looks at the content of ISPs and to what extent their updates are overdue for UK schools, this thesis looks at the update frequency and password policies for Swedish municipalities.

3.3 Delimitations

Due to the scale of the project, some delimitations were in place. Municipalities that required public documents to be handed out in person were only be obtained from the Västra Götaland region, as this was the place of operations for the authors. If the documents were required to be sent by letter and with a fee attached to it, as stated as a possibility in chapter 2 § 1 of the *Swedish Freedom of the Press Act* (TF, Tryckfrihetsförordning, SFS 1949:105), payment for the fee would have been taken out of a pool of 1,000 SEK. No further documents would have been acquired in this way, if that pool had been emptied within the duration of the project. The authors did not evaluate the security of the password policies themselves, only if the policy follows published

recommendations. The study aims to document the requirements for a municipality worker without special access to fulfill their work. Administrators or personnel within the education or healthcare sector are therefore excluded.

4 Methodology

In this chapter, the choice of method is presented and argued for. It also describes how the analysis and the data collection was executed. In addition to this, it also presents possible validity or reliability concerns and discuss the ethical issues of this thesis, deriving from the choice of methodology.

4.1 Choice of Method

Several methods could have been implemented to acquire the desired results: interviews, surveys, or document analysis, which is the process of examining and interpreting documents. Braun and Clarke (2013) stated that interviews are ideally suited for research on experiences but also useful in exploring constructs. To get good interview responses, the authors also stated that the respondent require a personal stake in the question to be able to produce a rich response. As the respondents' relation to the password policies would be a professional one instead of a personal one, and as this thesis did not intend to explore experiences or constructs, this method was rejected. The authors recommended surveys for topics in which the respondent does not have a personal stake in and stated that surveys are a quick and cheap way – in terms of both time and effort – to collect a lot of data. The authors also stated that surveys are ideal for sensitive topics as they provide some level of privacy and require less skill from the researchers to approach sensitive topics than other methods would. While the topic of password policies might be sensitive to some municipalities, the topic is not personally sensitive to the respondents. It was assumed that the authors refer to personal sensitivities, which means that the comment was not applicable to this study. Braun and Clarke (2013) also stated that surveys produce standardized answers compared to interactive methods, like interviews, which would be an advantage over the aforementioned method.

Bowen (2009) stated that the analysis of documents can be utilized to track changes and development, which is one of the key goals of this thesis. The author details seven advantages related to document research:

Efficiency: This method is more concerned with the selection of data rather than the collection of data. Gathering material for document analysis is generally much less time-consuming compared to other methods.

Availability: Documents within the public domain can easily be obtained quickly and without permission from the author.

Cost-effectiveness: The data within the documents has already been collected. All that remains for the researcher is to evaluate its contents and quality.

Non-obtrusive and non-reactive: The documents being analyzed cannot be influenced by the analysis process, meaning that the data within said documents do not change as a consequence of them being observed. A person being observed during an experiment may behave differently because they know that they are being observed. This is not an issue within document analysis.

Stability: Documents are stable by nature and may be reviewed repeatedly due to their contents staying the same.

Exactness: Documents tend to contain exact details regarding relevant names, references, and more, which is a general advantage.

Coverage: Documents can cover information from a broad span of time.

However, document analysis may suffer from the following disadvantages as well:

Insufficient detail: The documents being researched are not initially created with the intent of being used in research. They may, therefore, lack the details needed to answer a research question.

Low retrievability: Certain documents may be hard or impossible to retrieve. This is especially relevant for this thesis, as some municipalities may conclude that access to their password policies needs to be restricted.

Biased selectivity: The available documents are expected to have bias within them and do thus not represent reality in an unfiltered way. The documents may be angled to fit the agenda of a certain department or the organization as a whole.

It was deemed that the advantages heavily outweighed the disadvantages, not only due to the difference in the amount of advantages over disadvantages but also due to what they entail. The only disadvantage of any relevance to this thesis was low retrievability. The effects potentially created by low retrievability is explained in more detail in 4.4. Meanwhile, the advantages point towards this method being both efficient and a means to uphold the integrity of the collected data.

According to Atkinson and Coffey (1997, 2004, as cited in Bowen, 2009), researchers need to consider how documents in a document analysis serve the research purpose and that they should not be used as a replacement for other types of data. As this study aims to discover password policies through password policy documents, the statement has a high relevance to this thesis. While it is acknowledged that surveys would provide data tailored to this thesis with less uncertain variables, it was deemed that the risk of municipalities not responding was too high, which could invalidate the study due to a small sample size.

4.2 Data Collection

According to the *Swedish Freedom of the Press Act* (TF, Tryckfrihetsförordning, SFS 1949:105) chapter 2 §4, a document is part of the public record if it is kept in, created by, or received by a governmental agency. TF dictates that Swedish citizens have access to the Swedish public record, as stated in chapter 2 §1 (SFS 1949:105), and the access can only be limited if it is required by the following criteria:

1. The security of the kingdom or its relation to another state or organization.
2. The central financial politics, monetary politics, or exchange rate policies of the kingdom.
3. Government agencies for inspection, control, or other supervisions.
4. The interest of preventing and prosecuting crime.

5. The common economic interests.
6. The protection of individuals' personal or economical condition.
7. The interest to preserve animal or plant species.

Non-Swedish citizens can have these rights limited if written in law as stated by TF chapter 14 §5 (SFS 1949:105), but as no such law is written as of writing, non-Swedish citizens have the same rights to the public record as Swedish citizens. This does not entail, however, that everyone has the same right to the same information. According to the TF chapter 2 §18 (SFS 1949:105), municipalities are allowed to research who the person requesting the information is and what their intent is, to the extent that the municipalities can make a judgment if items n.o. 1–7 in chapter 2 §4 (SFS 1949:105) apply to the requested document. If the municipalities deem that the document contains pieces of information that apply to any of the items, they can either deny the request or redact the sensitive information as stated in *The Public Access to Information and Secrecy Act* (OSL, Offentlighets- och sekretesslagen, SFS 2009:400) chapter 5 §5. If a municipality classified a certain document as being a part of the public record, it is considered legal to disclose that information according to TF, chapter 1 §1 (SFS 1949:105), as long as the public document was not acquired by working in public service, the document would disclose information classified under professional secrecy, or if Sweden would be in war or in immediate threat of war, the disclosure of information that could violate the security of Sweden, TF chapter 7 § 20 (SFS 1949:105). As the documents were acquired through proper channels, the first clause does not apply. As access to the documents would not be granted if they were under professional secrecy, the second clause does not apply. As Sweden was currently not in or in the immediate threat of war, the third clause does not apply.

Primarily, the data was acquired from the municipalities' own online document registry, when available. If it was available online, an e-mail was sent asking if the document is current and if an old revision could be sent if it was not published. If they were not available online, the standard procedure for requesting public documents was followed. A request was made for the documents to be sent by e-mail—which is a request they are not required by law to fulfill, as suggested by the absence of such a statement in the TF (SFS 1949:105) . If such a request was denied, a request was instead made for them to send it by letter. Municipalities are allowed to take a fee in exchange for a printed copy, as stated in TF chapter 2 § 16. As stated in section 3.3, if the total cost for acquiring policies would have exceeded $1,000$ SEK, no further policies would have been acquired via printed copies. To filter out exorbitantly expensive documents, an acquisition fee exceeding a cost of 50 SEK per policy would have been rejected. When a municipality deemed that the documents were in the public record but were sensitive enough to require the requester to be physically present to procure the documents, procurement would only be considered if the municipality in question is within the Västra Götaland region. If the municipality required a physical presence and were outside the Västra Götaland region, they would have been rejected. Both the latest password policy document and one revision before it was requested.

A municipality was excluded from this study if one of the five conditions were true:

1. The municipality did not provide an answer or fit any of the other inclusion or exclusion criteria before 17/4 (classified as "No response").
2. The municipality denied the data collection request.
3. The municipality stated that they did not have such a document and provided no other information.

4. The municipality stated that they use passwordless authentication and provided no information on previous practices.
5. The municipality sent a document containing no password policy information.

A municipality was included in this study if they:

1. Stated that the document found online was current.
2. Provided a document stating either their current or past password policy.
3. Provided an extract from a document stating their current or past password policy.
4. Stated that they did not have a password policy document but provided information on their password policy implementation.

All received documents that did not fit the exclusion criteria were assumed to be password policy documents, and all information received in which the respondent did not explicitly state that they had no password policy document were assumed to be extracts. If a document was provided but all relevant information was redacted, the request was marked as rejected. If the document did not contain password policy information, it was assumed that the municipality had no document.

4.3 Data Analysis

The documents were analyzed and coded using an inductive as well as a deductive approach. The date of the document was recorded, along with statements about the number of required character classes, password length, and expiration times, which were deductively coded and categorized. General statements were inductively coded and categorized. The same process was used for the historical documents, and these components and codes were then compared to the current iteration, and the changes between them were noted. The document extracts were then randomly sorted and given a unique name. Dataset 1 consists of two combined numbers (01, 02, 03...), and dataset 2 consists of two combined letters (AA, AB, AC...). For graphs that intend to present a representative average, Tukey's Fences with $k = 1.5$ was used to calculate the outliers. Tukey's Fences is calculated by taking the distance between the lower quartile and the upper quartile in a set of values and multiplying it with k. Values found to be outside the quartile by this value are deemed to be outliers. As box plots are sensitive to outliers and can skew averages, the outliers were removed from the calculation to present what could be expected. All instances of outliers have been documented and presented.

4.3.1 Intercoder Reliability

Intercoder reliability is achieved when different coders would code the same data the same way (Campbell et al., 2013). The authors describe that a requirement for achieving intercoder reliability involves coders coding the same data the same way while operating independently and isolated from each other. For the coders to effectively code independently, a codebook was created that defined the different codes based on agreed definitions of the codes. The codebook can be seen in sections 5.2 and 5.3. After the independent coding was performed, a comparison was made between the coded data. As inspired by Gerlitz et al. (2021), Cohen's kappa coefficient was utilized to calculate reliability between the coders. McHugh (2012) stated that Cohen's Kappa

	Yes	No	
Yes	10	5	15 (62.5%)
No	7	2	9 (37.5%)
	17 (71%)	7 (29%)	

Table 4: An example for a table used in a Cohen's Kappa calculation. The X axis represents the answers from rater 1, while the Y axis represents the answers from rater 2.

is a widely used tool for measuring the inter-rater reliability between two coders. The value κ can range from -1 to +1, with +1 being perfect agreement between the raters beyond what could be expected by chance, 0 being the same distribution as if it was selected by random chance, and -1 being perfect disagreement beyond what could be expected by chance. To calculate the value, the number of agreements and disagreements must first be documented. See Table 4 for an example. In this table, there are two raters documenting responses as either a "Yes" or "No"—with rater 1 on the X axis and rater 2 on the Y axis—evaluating a total of 24 responses. Cohen's Kappa calculates how likely it is that these answers were given by random distribution based on the raters' predisposition to document a certain response. The level of actual agreement must first be calculated based on the amount of cases that both raters agree, divided by the total amount of responses. Both raters agree on "Yes" 10 times and on "No" two times, meaning that the actual agreement is $12/24 = 0.5$. Then, a calculation must be made which presents the likelihood that both raters agree by random chance. Rater 1 chose "Yes" 15 out of 24 times (62.5%) while rater 2 chose "Yes" 17 out of 24 times (71%). The likelihood of both raters choosing "Yes" is $0.625 \cdot 0.71$, resulting in that there is a likelihood of 44.4% that both raters chose "Yes". This value is then added with the likelihood that both choose "No", $0.375 \cdot 0.29 = 0.11$, indicating a 55% chance of agreement due to randomness. As both the actual agreement level and the chance of agreement is known, κ can now be calculated with the given formula.

$$\frac{\text{Actual agreement - Agreement due to random chance}}{\text{Perfect agreement - Agreement due to random chance}} = \kappa$$

This would produce, with the values from the example table,

$$\frac{12/24 - 0.55}{1 - 0.55} = -0.112\kappa$$

indicating a slight disagreement between the raters beyond what can be expected by chance.

Agreements and disagreements were noted after the coding process, and the level of agreement was calculated using Cohen's kappa coefficient. If the level of agreement had been deemed to be below an acceptable level, coding would have been performed again from the beginning. Since the level of agreement was deemed to be sufficient, each of the instances of differing codes were analyzed in an attempt to conclude why they differ. When the differences were due to differing interpretations of the code book, the codes were redefined based on an agreed definition between the coders, and the statements were re-coded appropriately based on the new code definitions.

4.3.2 Research Question 1

By comparing the coded policies with the recommendations from NIST, MSB, IIS, and ENISA, the compliance rates were measured. For measuring the compliance rates of SUNET's requirements, the entropy value of the weakest password that can be generated using the password policy needed to first be calculated. This was done using the calculation presented in section 2.2.1.

4.3.3 Research Question 2

The effective date of the current policies was noted, and the policy's age was documented. The effective date of the previous policy was then subtracted from the effective date of the current policy, with the sum being the lifespan of the last revision. All the coded variables within the current policy were compared with the previous one, and changes were documented.

4.3.4 Research Question 3

The Pearson Correlation Coefficient and the Spearman Correlation Coefficient were used to measure the relationship between password length and the year of the policy's effective date. As Pearson measures a linear relationship and Spearman a non-linear one, the combination of these two values can be used to deduce an overall relationship. If both Pearson and Spearman are of a high value, this indicates that the relationship is linear. If Pearson is of a low value and Spearman is of a high value, this indicates that the relationship is non-linear. If both values are low, this indicates that there is no relationship at all (de Winter et al., 2016). The size of the correlation was evaluated based on the writings of Cohen (1977, pp. 413–414).

4.4 Validity and Reliability

Bias may be an influencing factor during the interpretation of the codes as they could lead to an inclusion or an exclusion of a variable that is not defined well enough. To alleviate this problem, the documents were coded independently by two raters as mentioned in section 4.3.1. This does not protect against a scenario in which both raters interpret the same ambiguous statement in the same way. As previously mentioned, a codebook was used, which helped resolve any differences encountered during coding. This tool can be of help in the first scenario, but for the latter, there is a risk that silently agreed-upon undocumented definitions have not been included.

Berndtsson et al. (2008) stated that the inability to account for bias can be an issue to the validity of a thesis. As mentioned in section 4.3, steps were taken to account for potential forms of bias from the authors. The intention of the thesis is to document the overall picture of the password policies used by municipalities in Sweden. There is, however, a possibility that an insufficient amount of policies was received to create a representative picture of the current state, mostly due to the low retrievability rate that correlates to the act of collecting documents in general. Furthermore, the current societal situation with Sweden experiencing an increase in cyber security attacks and influence operations, as well as an increase in activities that can be classified as collection attempts of sensitive information, see appendix C.

Municipalities being on high alert could further affect an already lowered retrievability rate. This may have led to the possibility of a volunteer bias. As specified in 4.2, access to the requested information can be denied if the municipality deems it inappropriate to comply with the data collection request. This can be perceived as municipalities having the option to opt in or opt out of participating in the study. One can then come to the conclusion that municipalities that have confidence in their IT strategy may be more likely to opt in than those who are less confident. This could possibly skew the data and result in an over-representation of confident municipalities. However, since the process of evaluating public documents cooperating with handing out public information is a legal obligation for Swedish municipalities, this risk is not as fully realized as it would have been in the case that participation was entirely optional.

It is a possibility that the risk that an insufficient amount of previous revisions were received in order to be able to make generalized statements about the changes between the revisions. Password policies were looked at and the revision rates were documented, but only one revision back as no older documents were requested. As such, it can not be assured that the revision rate has stayed consistent in past revisions or that it will continue to in the future. Conclusions that allude to such are out of scope for this thesis. Additionally, it can not be guaranteed whether any previous revisions received are the ones from one revision back, or simply an older one found. As such, any previous revisions received are assumed to be from one version back.

A potential threat was that the receiver of the request might have misunderstood what document was intended to be acquired and have sent the wrong one. If this has gone unnoticed, and a password policy for another department was received for example, the document would have been assumed to be within scope and processed as such. Another validity threat is that of the translation of Swedish laws and direct quotes from the password policies. Quotes and statements translated into English might not have had the same connotations as the original Swedish texts. To alleviate this concern, all translations have been peer-reviewed by an impartial third party. Yet another validity threat is the formulation of the e-mail requesting the data as this was used by municipalities to assume intent as to make a judgment if items number 1-7 in chapter 2 §4 (SFS 1949:105), as shown under 4.2, were applicable.

4.4.1 The Data Collection e-mail

As the municipalities' response time to e-mails were an uncertainty going into the data collection phase, the first e-mail written for the data collection requests was conceived in haste and without much consideration. This revision of the e-mail was sent only to municipalities within Västra Götaland Country. This first revision contained the following:

- An introduction of the authors
- A brief explanation of the thesis
- A description of the data that was sought after
- On what legal basis the documents were requested
- Closing words and "thank-yous"

It was revealed during the e-mailing process that the quality of the e-mail was not on par with what is expected of a formal data collection request. The quality of the e-mail may have had an impact on the willingness of a municipality to send a response. A second revision of the e-mail was drafted to avoid that possibility from reoccurring. The second revision drew inspiration from Indeed, which recommend a three-paragraph structure (Indeed Editorial Team, 2023). Paragraph one introduces the sender and includes the data request along with the intended use of the data. Paragraph two serves as an explanation as to why the data is needed and who else might see it. Paragraph three closes the mail, and thanks the recipient for their time. Much of this was missing from the first revision, and it became evident that an update was necessary. In addition to what was written in the first revision, the second revision added the following:

- A much more detailed description of the purpose of the study
- What will be published

- The process of the study and how the data was intended to be handled
- Contact information for the authors of the thesis and their supervisor
- A few semantic and spelling fixes

Both of the e-mail revisions can be found under Appendix A. Due to the first revision being seen as a blunder, it was deemed to be best to split the data into two sets. Dataset 1 contains only the data collected from the Västra Götaland region, while dataset 2 contains the data from every region in Sweden, sans the Västra Götaland region. These were analyzed independently of each other in order to avoid potentially inconsistent data as a consequence of the first e-mail revision. To measure the impact on the response rate of the revision, a *t*-test was performed between the response rates of the two groups, as the result may allude to whether the initial revision had an impact on the response rate or not.

4.5 Societal and Ethical Aspects

The timing of this particular study could be described as unfortunate. With cyber-attacks on the rise, as mentioned in section 2, and as was stated in the document sent out by Västra Götaland – see appendix C – data collection requests are on the rise as well. As such, public officials have every right to react with suspicion upon receiving a request for data collection. Discerning a data collection request for legitimate research purposes and one with malicious intent is nigh impossible. A more well-versed researcher could probably have been more successful in collecting and analyzing meaningful data than what is presented in this thesis, but the data collected and the conclusions made may still be useful for future research or as an argument for some action to be taken. If this thesis uncovers systematic password policy issues or unacceptably low compliance rates, regional politicians could potentially use this data to motivate a campaign in order to increase the security threshold or prompt MSB to release concrete guidelines and recommendations. Additionally, it is worth acknowledging the time spent by public officials in order for the requested data to be received. A data request e-mail was sent out to every single municipality in Sweden, regardless of whether their password policy document was available online or not. The collective amount of man-hours that had to be spent by every single municipality for this thesis project to be successful could merely be speculated. This is based on the presumption that every municipality likely had to forward the mail to the appropriate representative, perform an examination to evaluate whether it was appropriate to send back the requested information or not, and finally procuring the information and sending it back. Even refusals most likely went through a similar process.

Morgan (2022) states that a document analysis as a method raises fewer ethical concerns than other qualitative methods and continues that this is due to the fact that documents within the public domain are usually created with the intent of the general public reading them. As stated in section 4.2, while password policy documents were not created with the intent of being used by the general public, all documents created by municipalities that are not classified are part of the public domain. As documents within the public domain can be requested and retrieved by anyone, the creators of the documents should have had this in mind during the creation process. As such, being read and having data extracted from it might not have been the primary purpose of the document, but it is one that should have been considered.

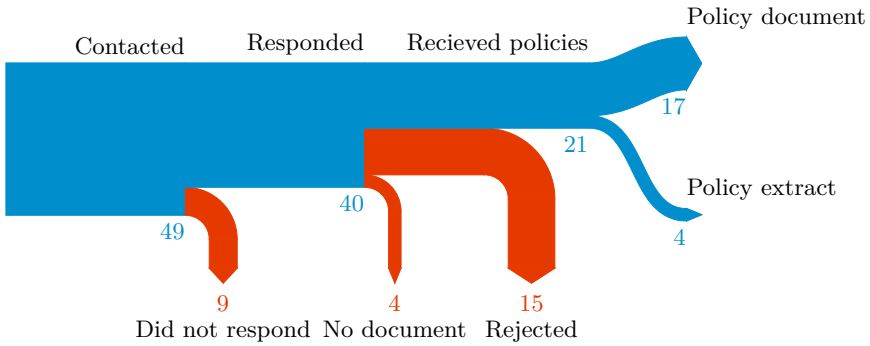

Figure 1: A breakdown of the response rates for Dataset 1.

5 Results

A summary of the data gathered is presented in this section. In section 5.1, the response frequency of the two datasets is shown, as well as the rejection rate and what form the received data took. In section 5.2, the deductive codes are presented, and in section 5.3, the inductive codes are presented. The data for the research questions is presented in their respective sections.

5.1 Data Gathering

For dataset 1, containing the municipalities in the Västra Götaland region, four password policies were found online. On February 23, the e-mail in appendix A.1 was sent out to all the municipalities in the Västra Götaland region. Approximately three weeks later, on March 14, the e-mail in appendix A.4 was sent to the municipalities that had not replied to the first e-mail. Out of the 49 municipalities contacted, 40 responded. Of these 40 replies, 15 municipalities rejected the data collection request, and four stated they had no documents to provide. Documents or document extracts containing password policy information were provided by 21 municipalities. Only eight municipalities out of these 21 provided historical documents. Of these 21 documents, four municipalities explicitly stated that they did not have a document describing the policy in place but provided information about the policy anyway, and 17 municipalities provided extracts from a document or the document itself. The acquisition rate for this dataset was 42.8%. See Figure 1 for a visualization of the responses.

For dataset 2, containing all the municipalities excluding the ones in the Västra Götaland region, 30 password policy documents were found online. Between March 19 and 21, the e-mail in appendix A.2 was sent to the municipalities with no documents published online, and the e-mail in appendix A.3 was sent to the municipalities with information published online. Approximately three weeks later, on April 9, the e-mail in appendix A.4 was sent to the municipalities that had not replied to the first e-mail. Out of 241 municipalities contacted, 173 responded. Out of these 173 replies, 31 municipalities rejected the data collection request, 28 municipalities stated that they had no documents to provide, and one municipality stated that they no longer used passwords for authentication. One municipality required the document to be viewed in person or sent by mail. As this municipality was not within Västra Götaland, and the printing cost exceeded the previously set boundaries, see section 4.2, the document was excluded from the study. Documents or document extracts containing password policy information were provided by 112 municipalities. Out of 112 municipalities, 36 of them provided historical documents. Of these 112 documents, 14 municipalities explicitly stated that they did not have a document describing the policy in place but provided information about the policy anyway, and

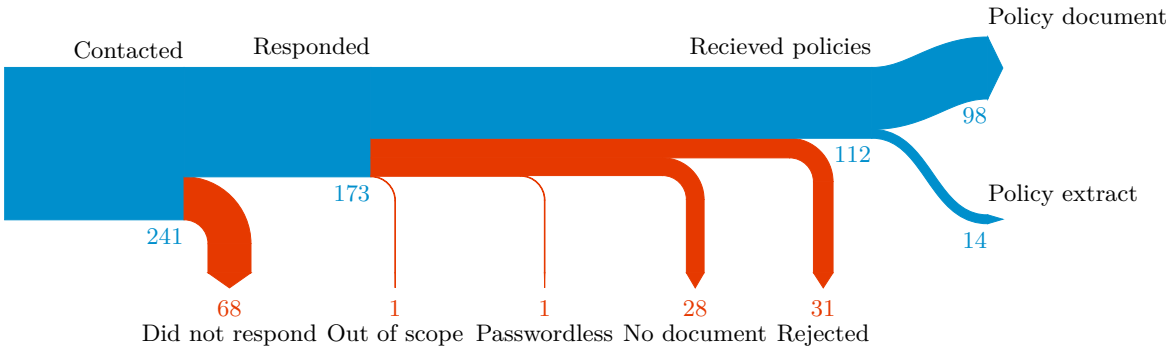

Figure 2: A breakdown of the response rates for Dataset 2.

98 municipalities provided extracts from a document or the document itself. One municipality rejected the request for information, but their password policy was later provided and had its status of being currently in use confirmed by another municipality. This document was included in this study and classified as receiving a policy document. The acquisition rate of dataset 2 was 46.5%. By analyzing the document acquisition rates between dataset 1 and 2 with the Student's T-test, the value of 0.645 was calculated, indicating there is a 64.5% chance the differences in the acquisition rate are due to variables other than the formulation of the e-mail (Gosset, 1908). As this value is larger than $\alpha = 0.05$, the null hypothesis for the e-mail's impact on the response rates cannot be rejected. See Figure 2 for a visualization of the responses.

5.2 Deductive Coding

The variables in the deductive coding mostly contain numerical data, but values may also be missing or undefined. These have been treated differently, as the complete absence of a code does not equate to a code that does not have a specified value. If a policy alludes to the presence of a variable but does not define an actual value, it has been coded as "undefined." A policy that does not mention a certain code is considered missing data and has been coded as "n.a.". Instances of undefined and missing values count towards the total number of mentions. However, they have been excluded from calculations, such as averages, due to the values not being equal to zero or any other integer values. A few policies specified the absence of certain variables. In those cases, the value is "no" to signify that the value is explicitly absent. The same applies here as with undefined and missing values. A value of "no" is not equal to an integer and is therefore not counted towards the number of mentions. A value must be an explicit requirement according to the password policy for it to be coded. Recommendations or "soft" requirements have not been included and are counted as missing. Any dates have been noted, and only the year is presented. The following list represents the deductive codes as they were written in the code book with examples taken from the municipalities policies:

Minimum length: The minimum number of characters a password must have to be considered valid.
Example: "The password shall consist of at least 8 characters."

Number of character classes: The number of character classes that a password must include within a password to meet complexity criteria. A policy that requires using uppercase characters but doesn't state anything regarding lowercase characters may imply that the use of lowercase is implicitly included. However, as this is an uncertainty, no character classes are counted unless they are explicitly mentioned.

Example 1: "Your password shall consist of at least 14 characters in which both minuscule (lower case letters) and majuscule (upper case letters) characters are used."
Example 2: "The password shall contain characters from 3 out of 4 categories."

Login failures before lockout: The number of failed login attempts allowed before the user is timed out from trying again either for a set amount of time before a new set of attempts is granted or is locked out indefinitely.
Example: "After three failed login attempts, the account is locked."

Days between forced password change: The number of days a password is valid before the system forces the user to create a new password.
Example 1: "Password changes are scheduled every 30 days for the internal network. A dialog popup will show up on the screen when it is time."
Example 2: "The IT-systems in production shall be able to force a password change on demand (immediately) or within a set time frame."

Password history: The number of previously used passwords per user that are saved in memory and can't be reused until it is rotated out of memory. Some policies have set this requirement to a specific time frame rather than an amount. These are treated almost the same but have the time frame specified as the number of days, months, or years when applicable.
Example 1: "Not the same as the last 24 passwords."
Example 2: "Not reuse the same password within 1 year."

Minimum character change between passwords: The minimum number of characters that must be different compared to a previously used password in order to be valid. Some policies specify that more than the last character must be different compared to a previously used password. Such a statement is a special case, as it concerns the position of the character rather than the number of characters. Such statements are coded as "1*".
Example 1: "Must differ from the last password with more than the last character."
Example 2: "At least four characters must be changed during a password change."

Effective date: A policy document's effective date, presented as a year. If more than one date is found within the document, the order of priority is as follows:

1. The date of the last revision
2. The date when the document came into effect
3. The date when the document was written

Example 1: "Date 2019-10-16."
Example 2: "Established 2023-09-20 by the head of IT."

Validity period and revision interval: The date when the policy document stops being valid, how often the document is revised, or how often the document is considered for review. Since no policies contained more than one of the specified options, there was no need to consider an order of priority. If the document is valid until further notice, it is coded as such.
Example 1: "Period of validity: Until further notice + First review 2022-09-01."
Example 2: "Valid until 2026-12-31."

5.3 Inductive Coding

For the inductive coding, statements that did not fit the predefined categories were extracted and analyzed. The following list represents the inductive codes as they were written in the code

book with examples taken from municipalities policies:

Disallow Unicode-characters: Often written as disallowing the usage of the characters å, ä, and ö but can sometimes be referred to as non-English characters. It has also been expressed as forbidding the usage of diacritic characters.
Example 1: "Capital letters [A-Z]."
Example 2: "Avoid the use of å, ä, or ö in passwords."

No personal info: A written statement that disallows the usage of personal info in the password creation process.
Example 1: "Passwords shall not contain the user's first name, last name, username, e-mail, or other pieces of information that can easily be connected to the user."
Example 2: "Avoid passwords that can be associated with your person."

No sequences or patterns: A statement that disallows using a certain number of repeating characters or sequential patterns.
Example: "Simple, repetitive patterns, for example ABCD1234, AAAAAAA2 shall be avoided."

Blocklist dictionary words or common passwords: A statement that disallows the usage of common passwords or dictionary words.
Example 1: "Do not use the words fotboll, losenord, password, hej, hejsan as a part of the password."
Example 2: "Do not use the name of the season or its number."

Multi-factor authentication with password: Multi-factor authentication with passwords is defined as a statement requiring every worker to use an additional authentication method in addition to a username and password to authenticate themselves regardless of their position and the task to be performed. Statements that did not indicate MFA as a requirement were excluded. Additionally, statements regarding the requirement of using MFA that only were applied to a specific category of employee, as seen in 3.3, were excluded.
Included example 1: "MFA-multifactor authentication is activated for all personnel."
Included example 2: "Windows Hello is activated as standard."
Excluded example 1: "Users who work remotely identify themselves with a username, and authenticate themselves with a password and with a code for their own personal device (2-factor authentication)."
Excluded example 2: "Additional methods for signing in can be the use of bank-id or mobile bank-id, or safe cards, for example SITHS-card."
Excluded example 3: "Depending on the security classifications of the system, other requirements can be applied for login. For some systems, two-factor authentication is required which implies that in addition to a password, an sms needs to be received with a code for logging in, for example."

Safe to write down: A statement that disallows users from writing down the password to either a physical or digital note. This category has two values: "No" when it is never allowed to write it down, and "Safe" if it is allowed but requires the user to store the note safely.
Example for "safe" 1: "Passwords shall be handled as an important document."
Example for "safe" 2: "Do not write the password down if you cannot store it safely."
Example for "no": "Do not write your password down anywhere."

5.3.1 Statements Excluded from the Inductive Coding

Some statements were mentioned by so many municipalities that they were considered as obvious and were consequently deemed as trivial security practices. One statement was not mentioned by enough policies to be considered significant. The statements which were excluded are as follows:

Change the password if it has been exposed: This was considered obvious and a trivial security practice.

Do not share the password: Obvious. A trivial security practice.

Do not save the password in the browser. Obvious. A trivial security practice.

Passwords should be unique: Obvious. A trivial security practice.

The number of times a password can be changed daily. Very few policies mentioned this requirement.

Minimum amount of days between password change Very few policies mentioned this requirement.

5.4 Inter-rater Reliability

Cohen's Kappa was calculated between the codes of the raters. As per the brackets definition in Table 5, one code had no level of agreement (MFA w/ password), two codes had a weak level of agreement (Write down, Minimum number of changes), seven codes had a moderate level of agreement (Character classes, Number of failures before lockout, Forced change, Password History, No personal info, No sequences or patterns, Blocklist), one code had a strong level of agreement (Disallow Unicode), and one code had an almost perfect level of agreement (Minimum length). See Figure 3 for the codes and their agreement levels. It is worth noting that even though the code "MFA w/ passwords" reached a level of agreement of "None" as suggested by κ, the code had an agreement rate of 91% between the raters without including randomness in the calculation. This low score is due to Kappa accounting for weighted randomness and disregarding the large number of times the raters agreed on the coding, as the outliers were not consistently coded the same between the raters to not suggest the agreements were not due to random chance. The pooled kappa, as presented by Vries et al. (2008) had a score of $\kappa = 0.715$. All the conflicts between the raters were ultimately resolved by reviewing the codes with differing variables and re-coding them.

5.5 Policy Content

The following section presents the categories found during the coding process and presents the occurrence of the code as well as the distribution of the values within the current policies.

Value of Kappa	Level of Agreement	% of Data that are Reliable
0–0.20	None	0–4%
0.21–0.39	Minimal	4–15%
0.40–0.59	Weak	15–35%
0.60–0.79	Moderate	35–63%
0.80–0.90	Strong	64–81%
Above 0.90	Almost Perfect	82–100%

Table 5: An interpretation of Cohen's kappa.
Note: Adapted from "Interrater reliability: The kappa statistic" by M. McHugh, 2012, Biochemia medica : časopis Hrvatskoga društva medicinskih biokemičara / HDMB, 22, 276-82. Copyright 2012 by Croatian Society of Medical Biochemistry and Laboratory Medicine.

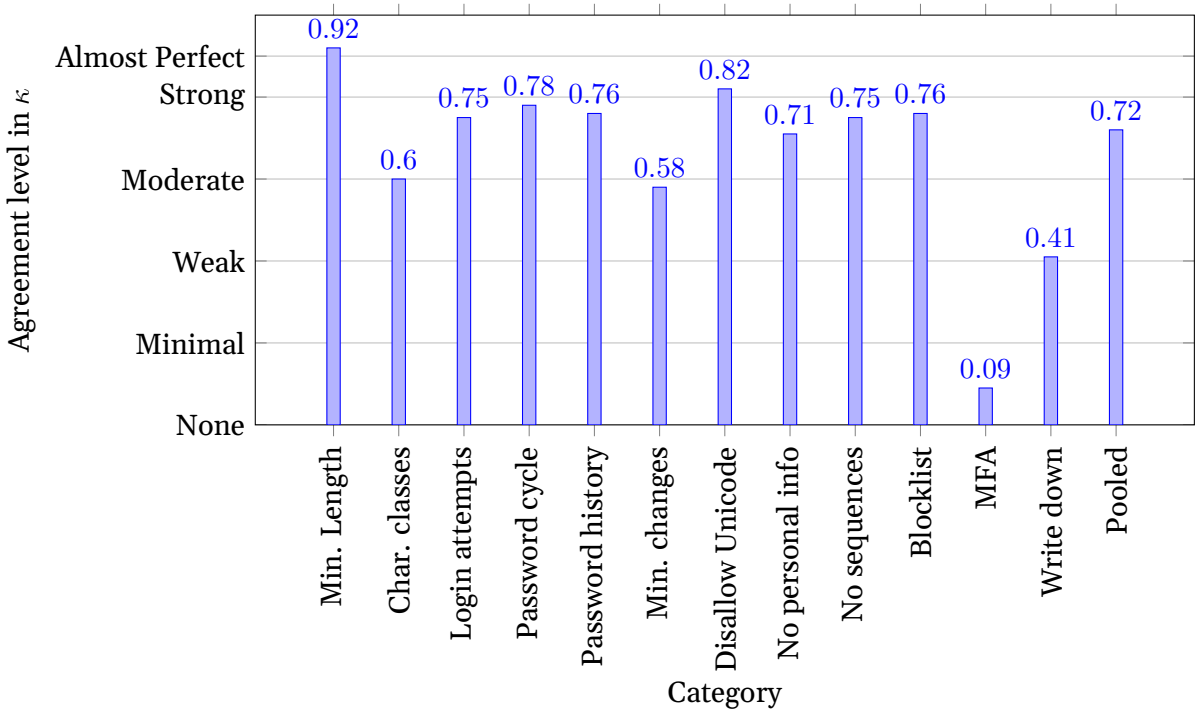

Figure 3: A bar graph showing the level of agreement for the different categories.

5.5.1 Password Length

Dataset 1 Out of the 21 current password policies analyzed for dataset 1, 19 (90.5%) had an explicitly stated minimum length. For minimum length characters in dataset 1, 16 municipalities (76.2%) had a policy of eight minimum characters, and three municipalities (14.3%) had a minimum requirement of 12. See Figure 4.
Dataset 2 Out of the 110 current password policies analyzed for dataset 2, 104 (94.5%) had specified a minimum length. For dataset 2, 39 municipalities (35.5%) had a policy of eight characters of length, 30 municipalities (27.3%) had a length of 12, and 11 municipalities (10%) had a length of 14. One municipality had three alternatives for their minimum password length which dictated how often the user was forced to change their password, with a shorter password requiring more regular changes. The changing variables between these alternatives are the minimum length. This municipality is represented by 8/10/12 to indicate their three different minimum password lengths. Overall, these three requirements accounted for nearly 75% of

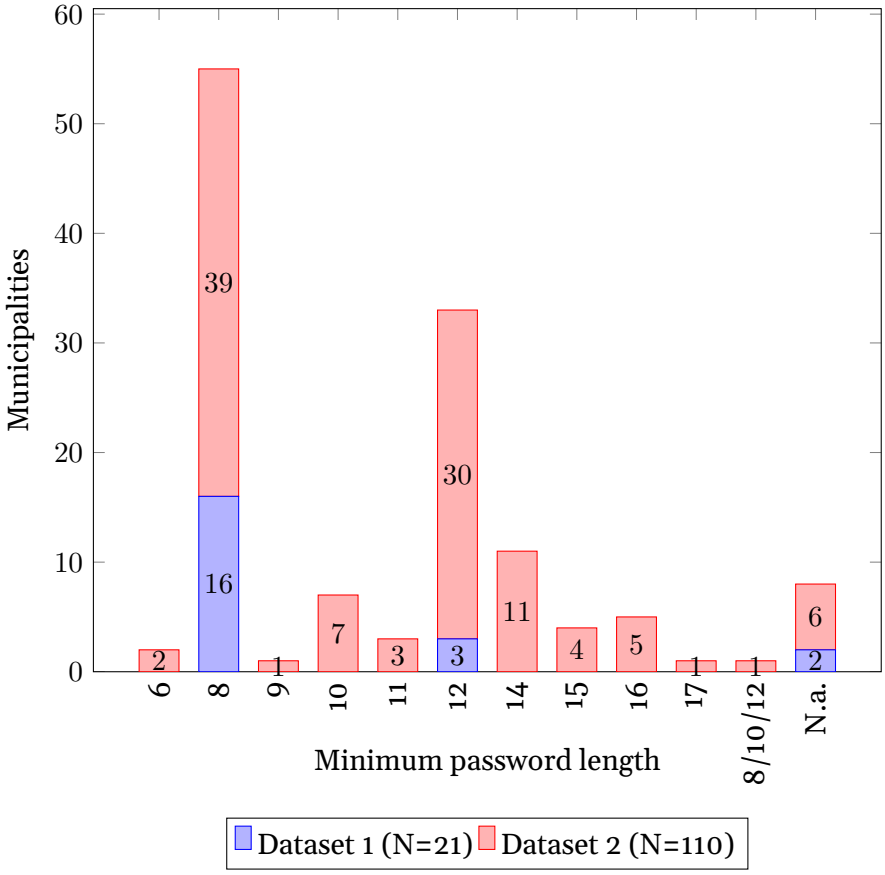

Figure 4: A bar graph showing the frequency of the minimum length value of dataset 1 and 2. 8/10/12 correlates to a code that provided more than one alternative for minimum password length.

all entries ($N = 110$). See Figure 4.

Combined dataset Out of 131 current password policies analyzed, 123 (93.9%) had specified a minimum length. Overall, 55 municipalities (42%) had a minimum length of eight, 33 municipalities (25.2%) had a length of 12, and 11 municipalities had a length of 14 (8.4%). See Figure 4.

5.5.2 Character Classes

Dataset 1 Out of the 21 current password policies analyzed for dataset 1, 17 (81%) had an explicitly stated minimum amount of character classes that needed to be present within a password. Sixteen municipalities (76.2%) required three character classes, while only one (5%) required two classes. See Figure 5.

Dataset 2 Out of 110 current password policies for dataset 2, 97 municipalities (88.2%) explicitly stated a requirement for using multiple character classes. Using three character classes was the most common with 61 municipalities (55.5%) requiring it, with 21 municipalities (19.1%) requiring four. Two municipalities (1.8%) explicitly stated that they did not force password complexity requirements. Fifteen municipalities (13.6%) either did not mention complexity requirements or stated that they did not use them. See Figure 5.

Combined dataset Out of 131 current password policies analyzed, 114 (87%) explicitly stated a requirement for using multiple character classes. The use of three character classes was required

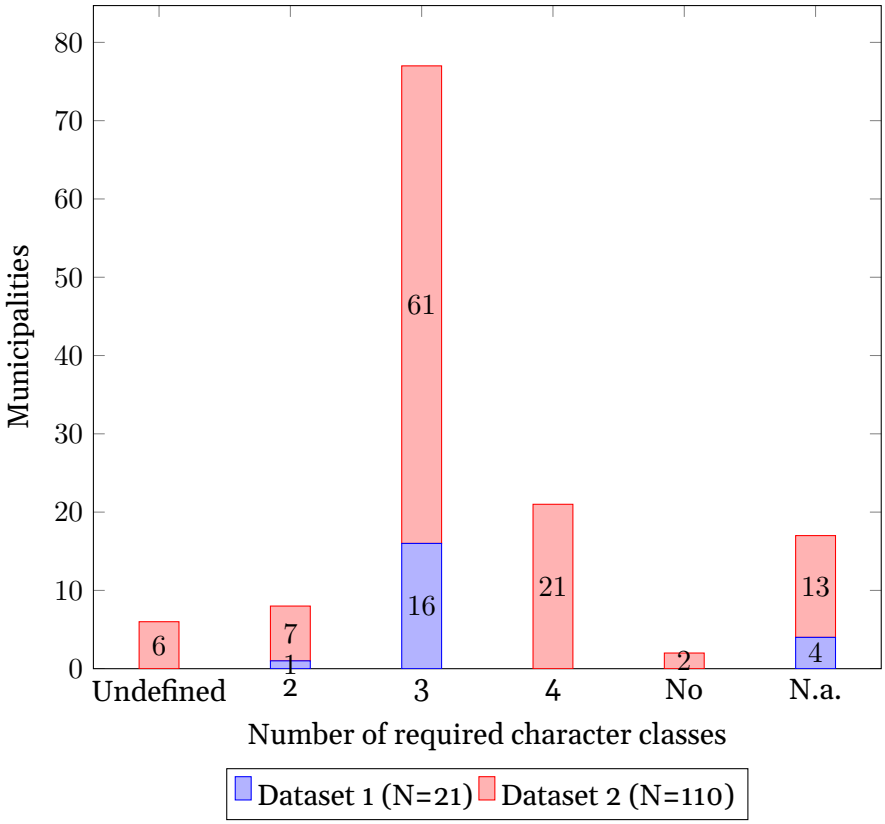

Figure 5: A bar graph showing the frequency of required character classes in dataset 1 and 2.

by 77 municipalities (58.8%), with 21 municipalities (16%) requiring four. Seventeen municipalities (14.5%) either did not mention a complexity requirement or explicitly stated that they did not use it. See Figure 5.

5.5.3 Login Attempts

Dataset 1 Out of 21 current password policies, 11 municipalities (52.4%) mentioned a lockout rule in the provided policy. Seven municipalities (33.3%) stated that users would be locked out after 10 attempts, with three municipalities (14.3%) having five attempts. Only a single municipality (4.8%) in dataset 1 allowed only three attempts before a lockout. See Figure 6.
Dataset 2 Out of 110 current password policies, 30 municipalities (27.3%) stated a lockout rule. Sixteen municipalities (14.5%) allowed for five attempts before a lockout, while seven municipalities (6.4%) allowed for three attempts. Five municipalities (4.5%) stated that a lockout would happen after too many attempts but did not specify a number. See Figure 6.
Combined dataset Out of 131 current password policies, 41 (31.3%) municipalities stated a lockout rule. Nineteen municipalities (14.5%) had a lockout rule set at five tries, while eight municipalities (6.1%) had it set to three tries. Five municipalities (3.8%) did not specify the number of tries. See Figure 6.

5.5.4 Days Between Forced Password Change

Dataset 1 Out of 21 current password policies, 13 municipalities (61.2%) had specified a maximum password age limit. Six municipalities (28.6%) had a variable limit between 180 and 270 days depending on the password length and complexity, while three municipalities (14.3%) had

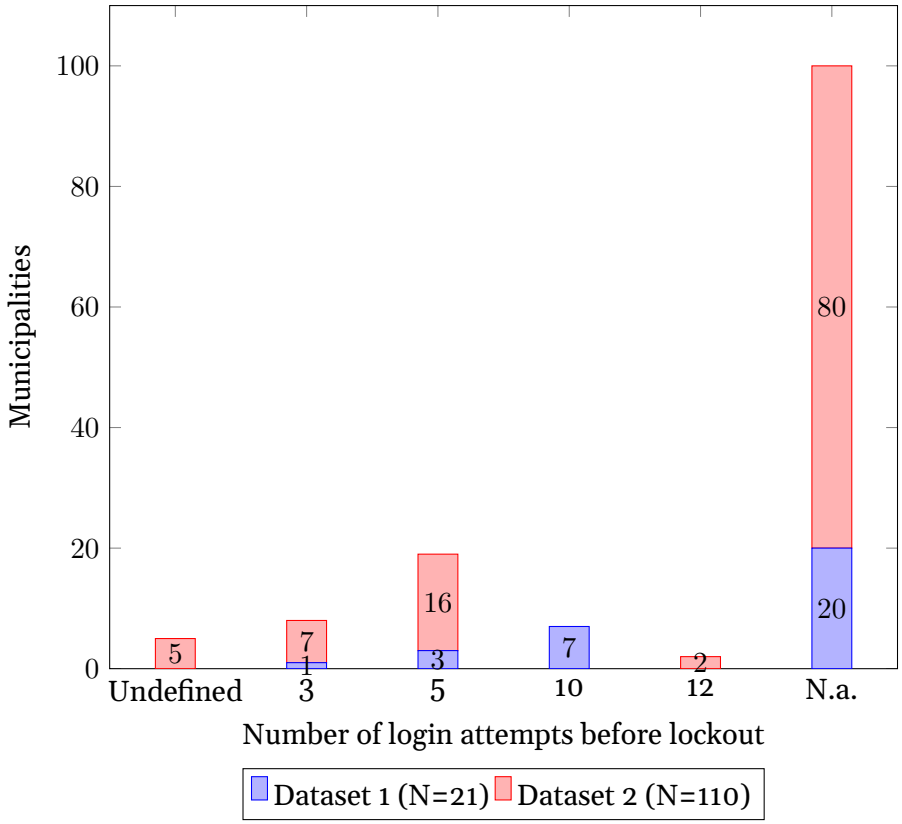

Figure 6: A bar graph showing the number of login attempts before a lockout in dataset 1 and 2.

a limit of 90 days. See Figure 7.

Dataset 2 Out of 110 current password policies, 80 municipalities (72.3%) stated that passwords expire. Having a password expiration of 90 days was the most common, with 20 municipalities (18.2%) adopting this rule. Twelve municipalities (10.9%) forced password changes every 180 days, with 11 municipalities (10%) forcing them once every 365 days. Thirteen municipalities (11.8%) stated that passwords expire but did not specify the number of days. Four municipalities (3.6%) explicitly stated that passwords do not expire. Overall, 34 municipalities (30.9%) either explicitly stated that they did not use password expiration or did not mention it in their policy. As mentioned in section 5.5.1, one municipality offered three alternatives for password length, which influenced how often users had to change their passwords. These alternatives are represented with the value 60/75/90. See Figure 7.

Combined dataset Out of 131 current password policies, 93 municipalities (71%) stated that passwords expire. Twenty-nine municipalities (22%) forced their users to change the password every 90 days, while 13 municipalities (9.9%) forced their users to change every 180 days. Eighteen municipalities (13.7%) forced their users to change passwords less than every 360 days. Forty-two municipalities (32%) either did not mention password expiration or explicitly stated that they did not use it. Only four municipalities (3%) explicitly stated that passwords do not expire. See Figure 7.

5.5.5 Password History

Dataset 1 Out of 21 current password policies, 14 municipalities (66.7%) specified that passwords could not be reused. Eight municipalities (38.1%) stated that a password could not be part of the previous 24 passwords, while four municipalities (19%) did not specify for how long the passwords could not be used. See Figure 8.

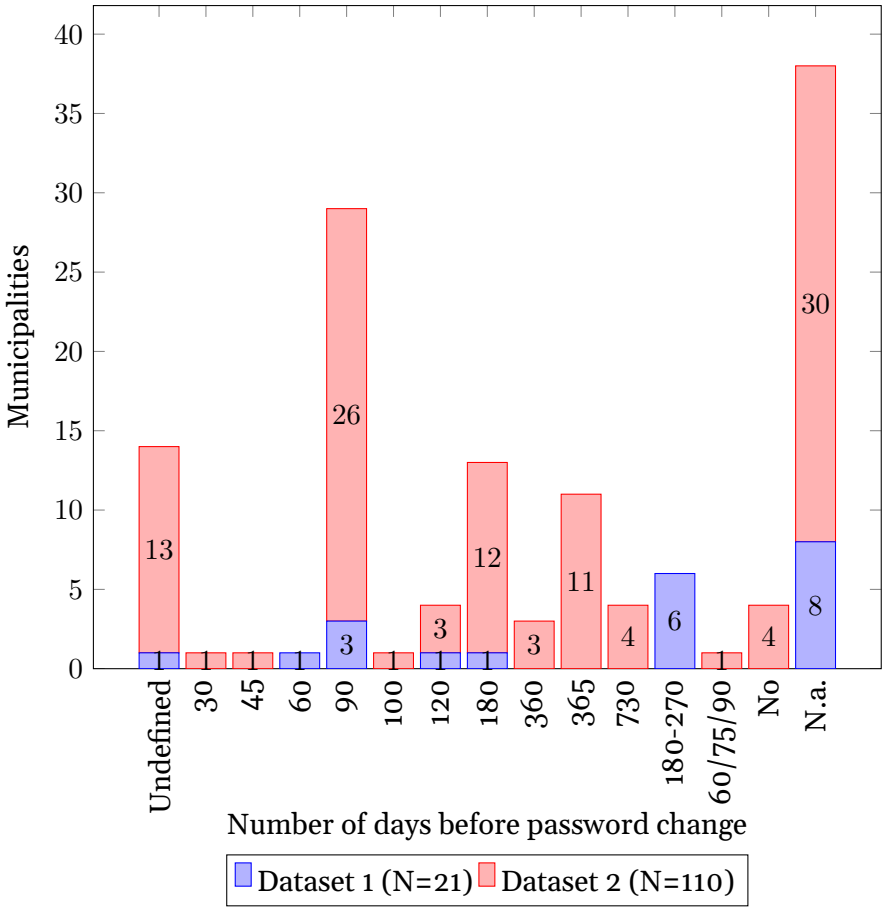

Figure 7: A bar graph showing the maximum password age in dataset 1 and 2. 8/10/12 correlates to a code that provided more than one alternative for maximum password age.

Dataset 2 Out of 110 current password policies, 61 municipalities (55.4%) had specified a password history. Thirty-six municipalities (32.7%) stated that passwords could not be reused but did not state a limit for how many previous passwords were checked. Twelve municipalities (10.9%) had a statement that they only check the 24 previous passwords. See Figure 8.
Combined dataset Out of 131 current password policies, 75 municipalities (57%) specified that password could not be reused. Forty municipalities (30.5%) stated that passwords could not be used but did not specify for how long, with 20 municipalities (15.3%) not allowing reusing the latest 24 passwords. See Figure 8.

5.5.6 Minimum Changes

Dataset 1 Out of 21 current password policies, seven municipalities (33.4%) specified a required number of character changes in comparison to previous passwords. Six of the municipalities (28.6%) required the change of one character that was not the last in the password. See Figure 9.
Dataset 2 Out of 110 current password policies, only 10 municipalities (9.1%) stated a requirement for the minimum number of changes between passwords. None of the codes that specified changes had more than a 3% usage. See Figure 9.
Combined dataset Out of 131 current password policies, only 17 municipalities (13%) stated a required number of minimum character changes between passwords. The most common statement was requiring that it was not enough to change only the last character, with eight municipalities (6%) requiring to do so. See Figure 9.

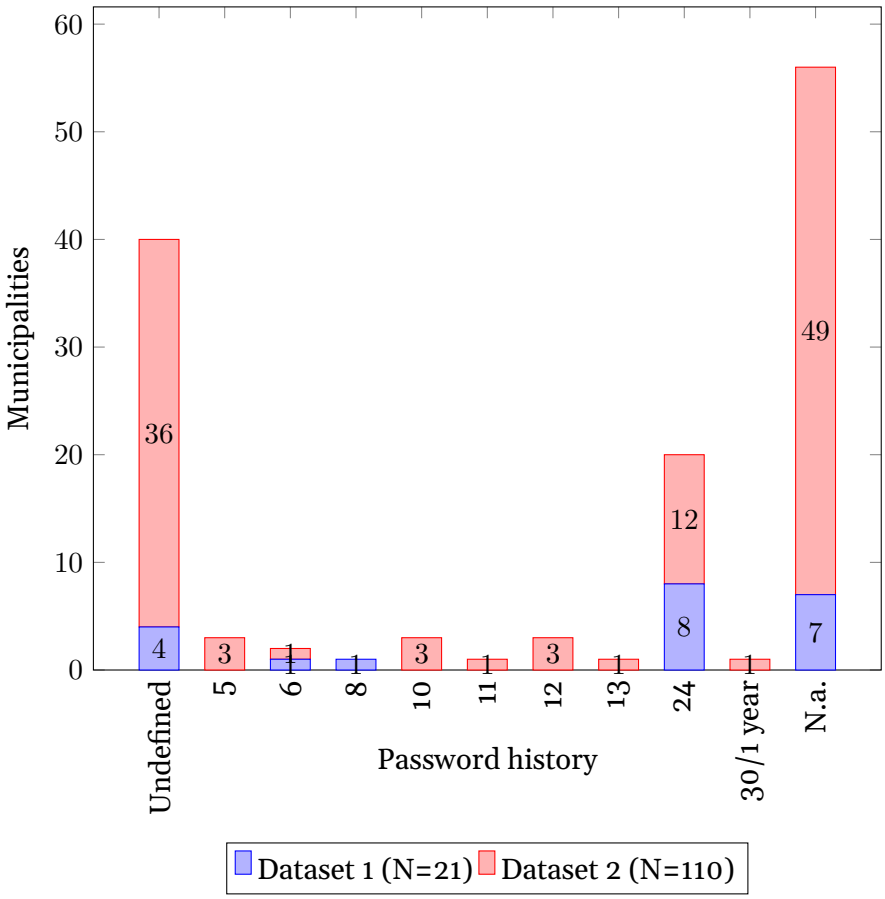

Figure 8: A bar graph showing the password history for dataset 1 and 2. ”30/1 year” correlates to a value which specifies that a password cannot be one of the last 30, or one created within the last year

5.5.7 Disallow Unicode Characters

Dataset 1 Out of 21 current password policies, 16 municipalities (76.2%) disallow the usage of Unicode characters. The remaining five municipalities either allow them to be used or did not mention the requirement (23%). See Figure 10a.
Dataset 2 Out of 110 current password policies, 33 municipalities (30%) disallow Unicode characters. The remaining 77 municipalities (70%) either allowed them to be used or did not mention it. See Figure 10b.
Combined dataset Out of 131 current password policies, 49 municipalities (37.4%) disallow Unicode characters. The remaining 82 municipalities (62.6%) either allow it or did not mention it. See Figure 10c.

5.5.8 No Personal Info

Dataset 1 Out of 21 current password policy documents, 18 municipalities (85.7%) had a statement disallowing the use of personal information in the creation of passwords, while three municipalities (23.8%) had no such statement. See Figure 11a.
Dataset 2 Out of 110 current password policies, 69 municipalities (62.7%) had a statement disallowing the use of personal information in the creation of passwords, while 41 municipalities (37.3%) did not. See Figure 11b.
Combined dataset Out of 131 current password policies, 87 municipalities (66.4%) had a

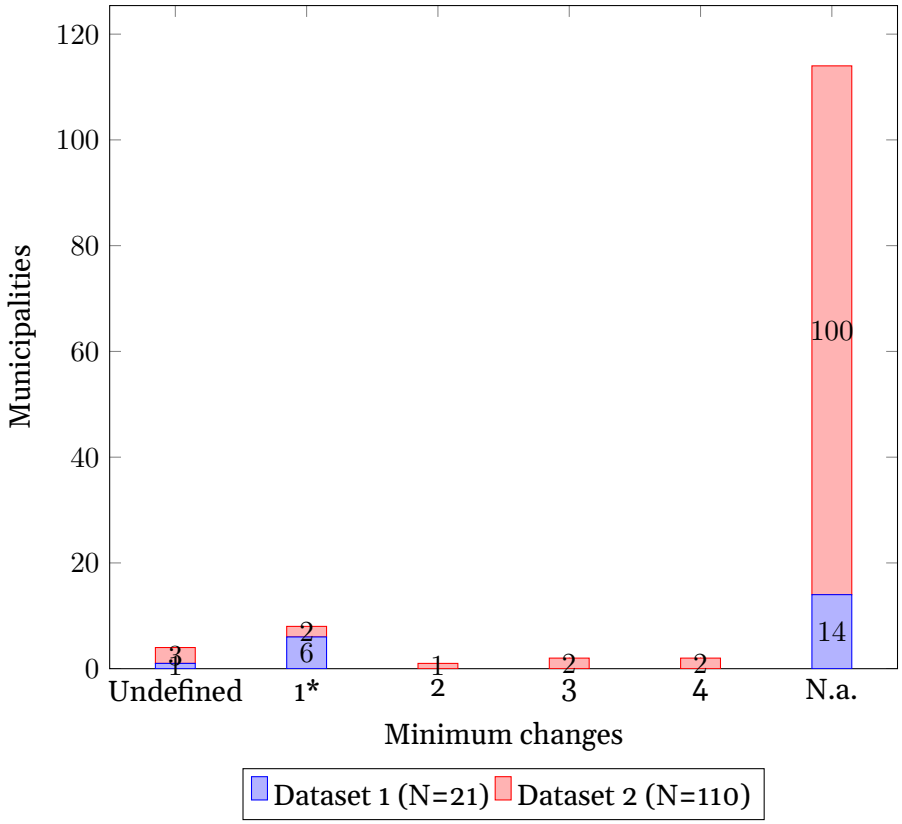

Figure 9: A bar graph showing the required number of changes between passwords in dataset 1 and 2.

statement disallowing the use of personal information in the password creation process, while 44 municipalities (33.6%) did not. See Figure 11c.

5.5.9 No Sequences or Patterns

Dataset 1 Out of 21 current password policies, nine municipalities (42.9%) had statements about not allowing repeating characters or patterns, while 12 municipalities (57.1%) did not. See Figure 12a.
Dataset 2 Out of 110 current password policies, 24 municipalities (21.8%) had a statement disallowing repeated characters, while 86 municipalities (78.2%) did not. See Figure 12b.
Combined dataset Out of 131 current password policies, 33 municipalities (25.2%) had a statement about disallowing repeated characters, while 98 municipalities (74.8%) did not. See Figure 12c.

5.5.10 Blocklist

Dataset 1 Out of 21 current password policies, seven municipalities (33.3%) disallowed users to use common words or passwords, while 14 municipalities (66.7%) had no such statement. See Figure 13a.
Dataset 2 Out of 110 current password policies, 28 municipalities (25.4%) disallowed users to use common words or passwords, while 82 municipalities (74.5%) had no such statement. See Figure 13b.

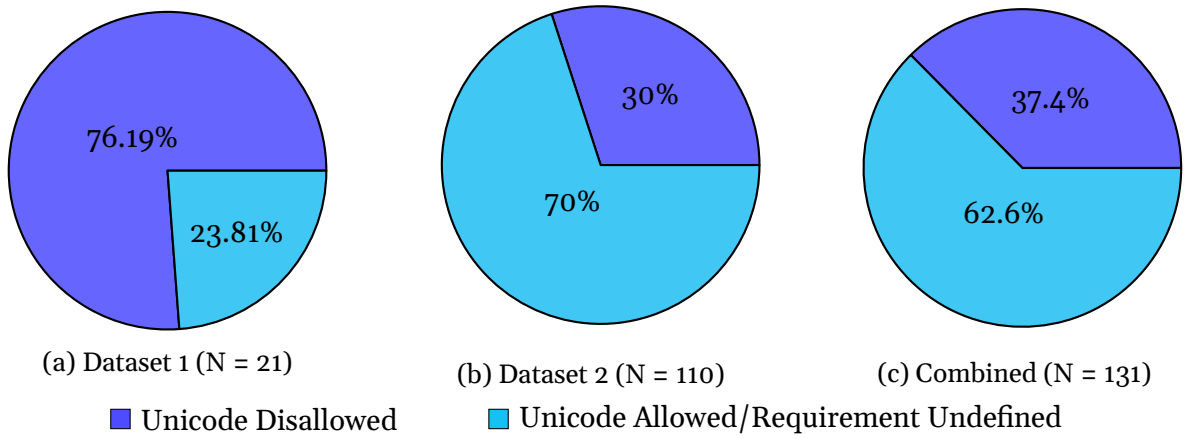

Figure 10: Pie charts depicting the percentage of municipalities that disallow Unicode characters within its user passwords in Dataset 1, Dataset 2, and the Combined Dataset.

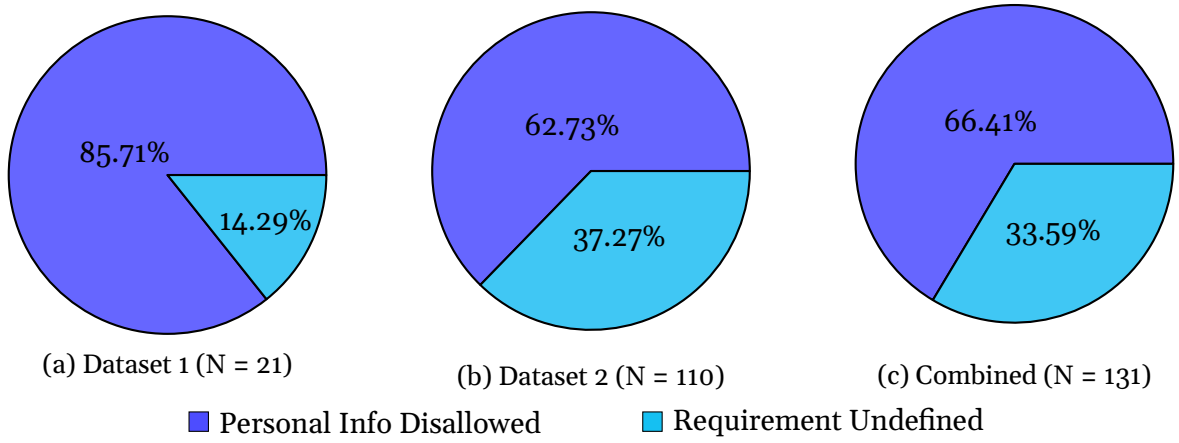

Figure 11: Pie charts depicting the percentage of municipalities that disallow user passwords that contain personal information in Dataset 1, Dataset 2, and the Combined Dataset.

Combined dataset Out of 131 current password municipalities, 35 municipalities (26.7%) disallowed users to use common words or passwords, while 96 municipalities (73.3%) had no such statement. See Figure 13c.

5.5.11 MFA with Passwords

Dataset 1 Out of 21 password policies, only one municipality (4.7%) required multi-factor authentication, with passwords being one of the authentication methods. The remaining 20 (95.24%) only enforced the use of MFA for users working from a distance, when handling sensitive information is involved, or included no statement regarding the use of MFA. See Figure 14a.
Dataset 2 Out of 110 password policies, only three municipalities (2.7%) required multi-factor authentication with passwords for all employees. The remaining 107 (97%) either did not require MFA at all, only while working remotely, or for accessing information requiring a higher level of security. See Figure 14b.
Combined dataset Out of 131 password policies, only four municipalities (3.1%) required multi-factor authentication with passwords for all employees, while the remaining 127 municipalities (96.9%) did not. See Figure 14c.

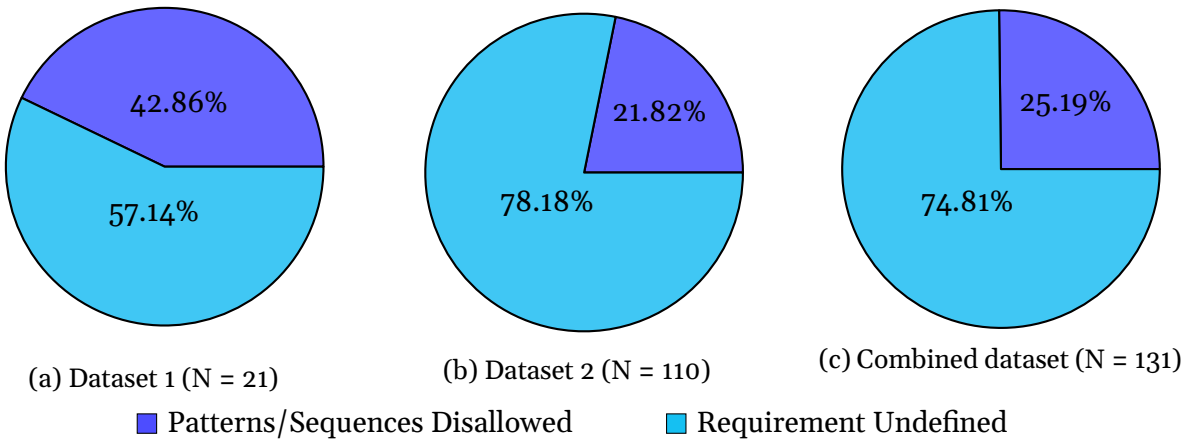

Figure 12: Pie charts depicting the percentage of municipalities that disallow user passwords that contain predictable sequences or patterns in Dataset 1, Dataset 2, and the Combined Dataset.

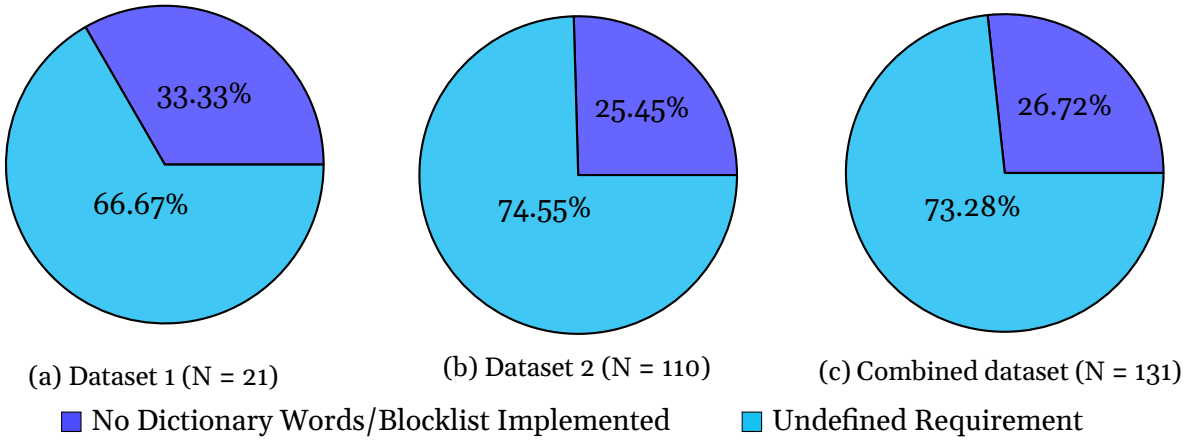

Figure 13: Pie charts depicting municipalities that disallow user passwords that contain words from a predefined blocklist and/or dictionary words in Dataset 1, Dataset 2, and the Combined Dataset.

5.5.12 Write Down

Dataset 1 Out of 21 current password policies, 10 municipalities (47.62%) explicitly stated that writing down passwords is strictly forbidden. Two municipalities (9.52%) either stated that it is allowed for passwords to be written down, or that they may be written down as long as they are not stored in proximity to their respective workstation and are handled with the utmost care. The remaining nine (42.86%) included no statement regarding the act of writing down passwords. See Figure 15a.
Dataset 2 Out of 110 current password policies, 15 municipalities (13.64%) explicitly stated that writing down passwords is strictly forbidden. Twenty-seven municipalities (24.55%) either stated that passwords are allowed to be written down, or that they may be written down as long as they are not stored in proximity to their respective workstation and are handled with the utmost care. The remaining 68 (68.82%) included no statement regarding the act of writing down passwords. See Figure 15b.
Combined dataset Out of 131 current password policies, 25 municipalities (19.1%) explicitly stated that writing down passwords is strictly forbidden. Twenty-nine municipalities (22.1%)

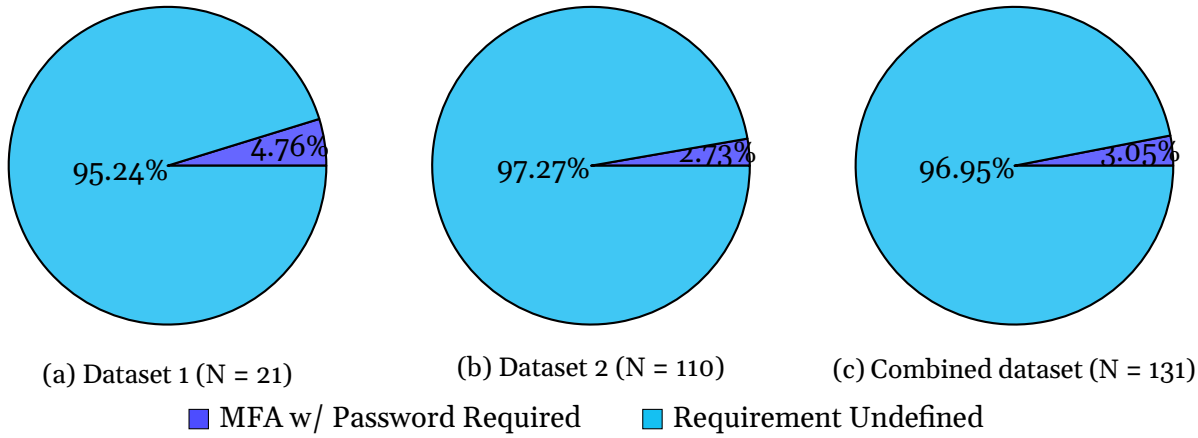

Figure 14: Pie charts depicting municipalities that require MFA to be used in addition to passwords for user authentication in Dataset 1, Dataset 2, and the Combined Dataset.

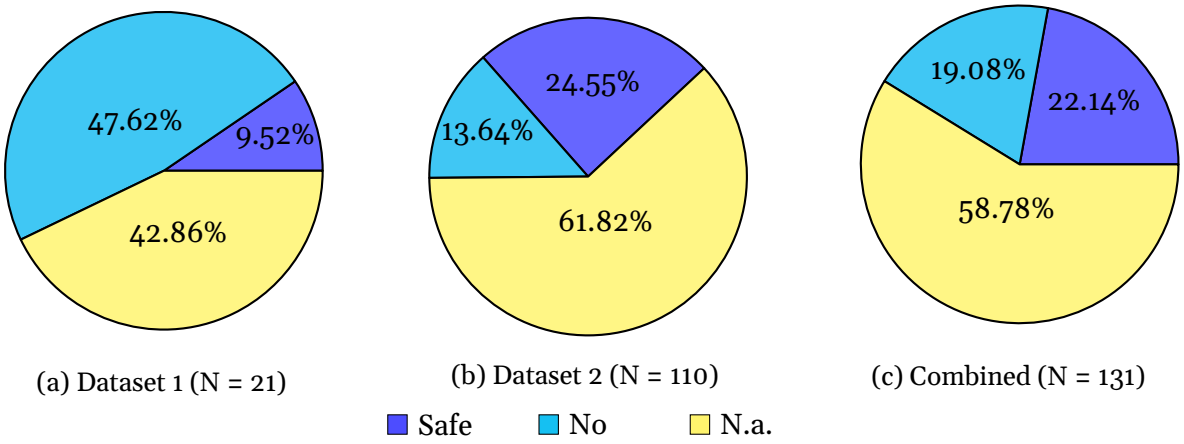

Figure 15: Pie charts depicting municipalities that have included statements regarding writing down passwords in Datasets 1 and 2 and the Combined Dataset.

either stated that it is allowed to write down passwords, or allowed but required the password to be safely stored. The remaining 77 municipalities (58.8%) had no statements about storing passwords. See Figure 15c.

5.6 RQ1: Compliance to Recommendations

This section provides the answer to research question 1. The observed recommendations for the organizations NIST, MSB, IIS, SUNET and ENISA is presented, along with how many of the municipalities that reached total compliance with said recommendations. Only concretely defined requirements are compared to the municipalities' password policies. Recommendations deemed "soft" or vague due to being encouraged or discouraged in contrast to more defined requirements and descriptions are listed but disregarded for the compliance check. Even a "hard" recommendation for multi-factor authentication is also be disregarded, as this authentication method is outside the scope of password authentication.

5.6.1 NIST

In NIST Digital Identity Guidelines SP 800-63-3, the recommended minimum length was specified as eight characters, with complexity requirements and regular password changes being discouraged. The use of multi-factor authentication was encouraged. See Table 2 for the recommendations.

For dataset 1, 19 current policies out of 21 (90.5%) were compliant with the recommendations provided by NIST. The municipalities that were not compliant, municipalities 01 and 11, did not have a specified minimum character length and were thus not compliant with the recommendations. For dataset 2, 102 of the current policies out of 110 (92.7%) were compliant with the recommendations. Most of the municipalities that were not compliant did not specify a minimum character length. However, two municipalities, municipalities BC and DO had a minimum character limit of six and thus fell below the recommended minimum of eight. For the combined dataset, the compliance rate was at 92.4%.

5.6.2 MSB

While having no concrete recommendations for password length and complexity, the organization does, however, write about factors that contribute to the generation of safe passwords, with the primary recommendations being blocklisting common words and disallowing the use of personal information in the password creation process, see Table 2 for the recommendations. For dataset 1, seven of the current 21 password policies were compliant with the recommendations. The policies that were not compliant did not disallow the usage of commonly used words and passwords. Only two policies disallowed common words or the use of personal information in the password creation process. For dataset 2, 27 of the current 110 password policies were compliant with the recommendations. All but one municipality lacked a statement about not allowing common words or passwords, with 43 municipalities lacking a statement about disallowing the use of common words and personal information. Municipality BK stands out as not being compliant even though they disallow common words; this is because they did not mention that personal information should not be used. For the combined dataset, the compliance rate was 26%.

5.6.3 IIS

The IIS states that passwords shorter than 10 are generally considered weak and that complexity is encouraged. Similarly to the recommendations by NIST, the IIS states that it is bad practice to change passwords that have not been compromised and that the use of sequences or common words within the password should not be used. While they state that it can be a good idea to write down passwords physically and safely store them, this is not a variable taken into the calculation as both values documented (Safe/No) fulfill this. See Table 2 for the recommendations. For dataset 1, none (0%) of the 21 current password policies fulfilled these recommendations. Six municipalities had statements about blocklists and not allowing sequences, but all of those six had a minimum length requirement of eight. Three municipalities had a length of over 10. However, none of them had statements about either blocklists or sequences. For dataset 2, 11 (10%) of the current 110 password policies were compliant with the recommendations. Out of those that were not compliant, six municipalities had statements about blocklists and sequences but had a password length requirement of less than 10 characters in length. Thirty municipalities had the required character length but lacked statements about not allowing sequences or common words. No municipality was excluded due to their policy not having a statement about

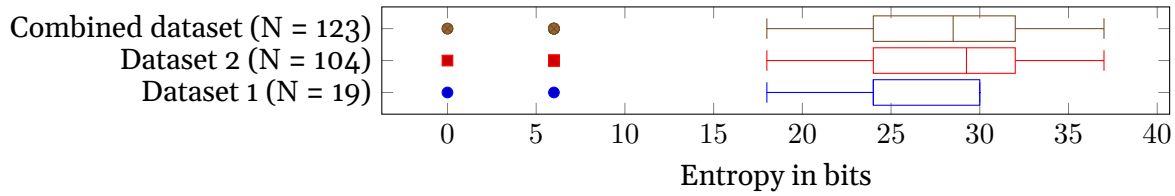

Figure 16: A boxplot over the estimated entropy value.

disallowing the use of personal information in the password creation process. For the combined dataset, the compliance rate was 8.4%.

5.6.4 SUNET

The requirements published by SUNET for reaching an Assurance level of 1 base a good password creation strategy on the concept of password entropy, as defined in NIST SP 800-63-2 (Burr et al., 2013). The entropy requirement placed by SUNET is 24 bits, and based on a password's length and complexity as well as the existence of a blocklist, see section 2.2.1 for the calculation and a table for the calculation, and Table 2 for the requirement. For dataset 1, 18 out of 21 municipalities were compliant by being over 24 bits. By using Tukey's Fences to analyze the entropy values, two outliers were found, one with the value zero and one with six. To not skew the data, these are excluded from the boxplot and the median. The median entropy was 24 bits, with the highest value calculated being 30 and the lowest being zero. For dataset 2, 101 out of 110 municipalities were compliant with the recommendations of being over 24 bits. Using Tukey's Fences, six outliers were found, one with a value of zero and five with a value of six. These are excluded from the boxplot and calculation to avoid skewing the data. The median entropy was 29.25 bits, with the highest value calculated being 37 and the lowest zero. The combined dataset had a compliance rate of 91.6%, with eight outliers, six of with had the value six and two with the value zero.

5.6.5 ENISA

The ENISA recommendations are defined as a password length of 15, with at least two character classes. Both personal info and sequences should be disallowed, and the password should not contain common dictionary words or weak passwords. See Table 2 for a summarization of the recommendations. Only municipality CQ in dataset 2 managed to reach total compliance with the recommendations set by ENISA. The compliance rate in dataset 1 is zero out of 21 municipalities (0%), and one out of 110 (0.9%) in dataset 2. The character length of 15 is not explicitly stated by ENISA, but the reason it has been defined as such is motivated in section 2.3.5. The unusually high length, combined with the other requirements, might be why the compliance rate is so low. Municipalities of note are AQ and AR, which achieved the length requirement but decided to opt-out from enforcing a complexity requirement, and municipalities like BF and CD which also managed to reach the length requirement but had no mention of a complexity requirement. Having a complexity requirement on top of a minimum length as high as 15 is unreasonable, as passwords created with these rules as a base tend to lead towards irresponsible user behavior instead. Municipality BJ sticks out, as it achieves ENISA's recommended password length and complexity, and explicitly states that users may not write down their passwords. This combination of requirements makes little sense, as it expects too much from its users who attempt to follow it. The remaining recommendations, as can be seen in Table 2 are reasonable, but only municipality CQ had all of these in mind in addition to the length

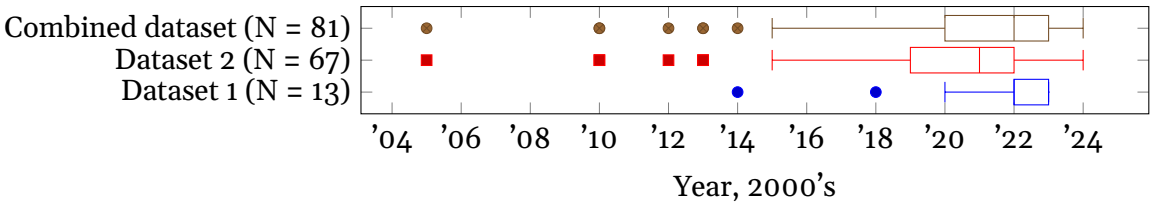

Figure 17: A boxplot over the effective date for the current password policies.

and complexity requirements. For the combined dataset, the compliance rate was 0.08%. It is worth noting that the ENISA recommendations is for the creation of a strong password, not for the exclusion of a weak one.

5.7 RQ2: Changes and Revisions

The following section answers research question 2, which looks at age and changes between revisions. Under section 5.7.1, the effective date of the currently used policies is presented. Under section 5.7.2, the validity period of the last policy is presented, and in section 5.7.3, the changes between the last policy and the current one are shown.

5.7.1 Current Policy Age

Of the current policies in dataset 1, 15 had a publication or a revision date. Using the Tukey's Fences algorithm for outlier calculation, two outliers were found, one dated 2018 and one 2014. For the 13 other policies, the median revision or publishing date was 2022, with 2023 being the upper quartile and 2020 being the lower. See Figure 17 for a detailed view. The median age for a policy with a specified publishing date, in dataset 1, was two years if outliers were ignored, with the oldest being six years old. It is worth noting that the oldest policy observed, municipality 16, featured both the currently most used values for minimum length and password complexity requirements at eight characters long, with three required character classes. Its longevity is possibly due to the policy being strong when created and still being on the lower end of what is currently being used nearly 20 years later.

Of the current policies in dataset 2, 73 had a publication or a revision date. Using Tukey's Fences algorithm for outlier calculation, six outliers were found. One of these outliers was dated 2005, two were dated 2010, one was dated 2012, and two were dated 2013. For the 67 other policies, the median date was 2021, with the upper quartile being 2022 and the lower quartile being 2019. See Figure 17 for more information. As per the oldest policy dataset 1, BQ from 2005, features a character length of eight and a complexity requirement of three, both being the most used within their category.

For the combined dataset, 88 documents or document extracts were analyzed. By using Tukey's Fences for outlier calculation, seven outliers were found. One from 2005, two from 2010, one from 2012, two from 2013, and one from 2014. For the 81 other policies, the median date was 2022 with the upper quartile being 2023 and the lower 2020.

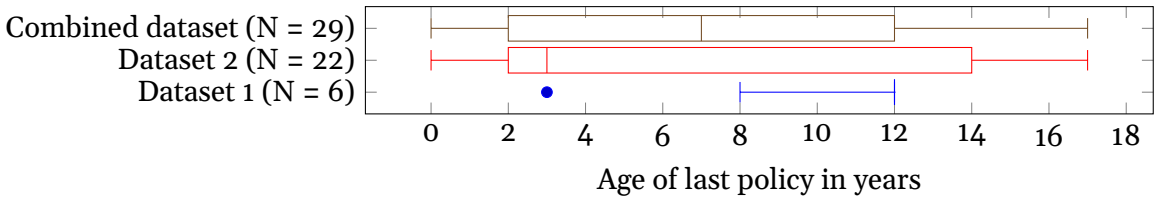

Figure 18: A boxplot representing the age of the previously used policies until a new version came into effect.

5.7.2 Previous Policy Age

The median age of the last policies used within dataset 1 was 12 years and had an average of 10 years. Using Tukey's fences algorithm shows one outlier, as seen in Figure 18. This outlier has a value of 3 years between the last revision and the current one. The median age of the last policies used within dataset 2 is 3 years and has an average of approximately 7 years. Dataset 2 contained no outliers. For the combined dataset, the median age was 7 years, with the youngest being 0 and the oldest being 17. The combined dataset contained no outliers.

5.7.3 Revision Changes

The codes of the current policies were compared to their previous revisions, and the data within Table 6 represents the percentage of areas that had undergone a revision represented by decimal numbers. The data in the table includes changes that both strengthen and weaken the overall quality of the password, as well as codes that were previously present but were removed in the next revision and vice versa. The following are observations of note regarding the changes made:

Dataset 1: There is not enough data to make any meaningful observations, this due in large part to the fact that six of the eight municipalities that provided a previous password policy revision have a shared IT-solution. See appendices B.1 and B.2 for details regarding the changes.

Dataset 2: Observing the changes to length within dataset 2 shows that a majority of the 67% that implemented a change between revisions increased the minimum password length. Of contrasting particular note is municipality DL, which instead had a decrease in length from 16 characters to 12 characters minimum. Municipalities CE and CN technically lowered their minimum lengths as well, as they now use an alternative solution for authentication. three municipalities had a defined complexity requirement in their previous policy but not in the most current one. Two municipalities that previously had complexity requirements explicitly stated in the current ones now state that they no longer require complex passwords. Eight municipalities previously had no defined complexity requirements but added them later. Two municipalities increased their complexity requirements from two to three, while one municipality decreased theirs from four to three. Most changes to login attempts regard either revision having no mention of the amount of permitted login attempts before lockout. Meanwhile, municipality CG increased the number of attempts from three to five. Six municipalities had differing defined numeric values in both provided revisions for forced password change, and all of them showed increased values, meaning that they forced their users to change their passwords less often than before. One municipality used to have a defined value but explicitly states that forced password changes no longer are used, while another municipality had no mention of forcing password changes but now explicitly states that it no longer is enforced. See appendices B.3 and B.4 for details.

Combined Dataset: In the combined dataset, almost 60% changed their length between revisions, with 64% changing their statements about expiring passwords. The most static category

Code	Dataset 1 (N = 8)	Dataset 2 (N = 36)	Combined (N = 44)
Minimum length	0.25	0.67	0.59
Character classes	0.25	0.44	0.41
Login attempts	1.00	0.22	0.36
Forced password change	1.00	0.56	0.64
Password history	0.88	0.36	0.45
Minimum changes	0.88	0.03	0.18
Disallow Unicode	0.88	0.31	0.41
No personal info	0.88	0.25	0.36
Sequences or patterns	0.75	0.17	0.27
Blocklist	0.75	0.22	0.32
MFA /w pass	0.00	0.03	0.02
Safe to write	0.25	0.25	0.25

Table 6: A table showing the percentage of policies which had the values of codes changed between the revisions represented by decimal numbers.

was MFA with passwords, which almost all municipalities continued not to have as a requirement.

5.8 RQ3: Age and Length

The trends between these two variables can be discovered by analyzing the relationship between the value revision date and the value length. For this calculation, both the current and old policies with specified dates and lengths were used, giving dataset 1 a sample size of 22 and dataset 2 a sample size of 92 policies.

For dataset 1, Pearson's correlation coefficient returns a value of 0.225, which indicates a small positive linear correlation. The P-value of Pearson was calculated to $P = 0.34$, indicating a 34% risk the linearity was due to standard deviation. As this value is higher than $P = 0.05$, the null hypothesis cannot be rejected, rendering this finding insignificant. Spearman's correlation coefficient returns a value of 0.346, indicating a medium positive correlation between the values. The P-value of Spearman was calculated to $P = 0.135$, indicating a 13.5% risk that the correlation value is due to standard deviation, thus rendering the finding insignificant. As Spearman is larger than Pearson, the relationship between age and length is more non-linear than linear. However, as the sample size is so small, the P value is large, and Tukey's Fences calculates the only non-eight value as an outlier, this result is ultimately considered unreliable. See Figure 19.

For dataset 2, Pearson's correlation coefficient returns a value of 0.509, which indicates a large positive linear correlation. The P-value of Pearson was calculated to $P = 2.198 \cdot 10^{-7}$, allowing the null hypothesis to be rejected. The Spearman correlation coefficient returns a value of 0.577, which indicates a large correlation between the values. The P-value of Spearman was calculated to $P = 1.707 \cdot 10^{-9}$, allowing the null hypothesis to be rejected. This dataset contains no outliers, according to Tukey's Fences. The relationship is mostly linear as both Pearson and Spearman indicate a high correlation coefficient. See Figure 20.

For the combined dataset, the Pearson correlation coefficient returns a value of 0.468, which indicates a medium positive linear correlation. The P-value of Pearson was calculated to $P = 1.903 \cdot 10^{-7}$, allowing the null hypothesis to be rejected. The Spearman correlation coefficient returns a value of 0.533, which indicates a large correlation between the values. The P-value

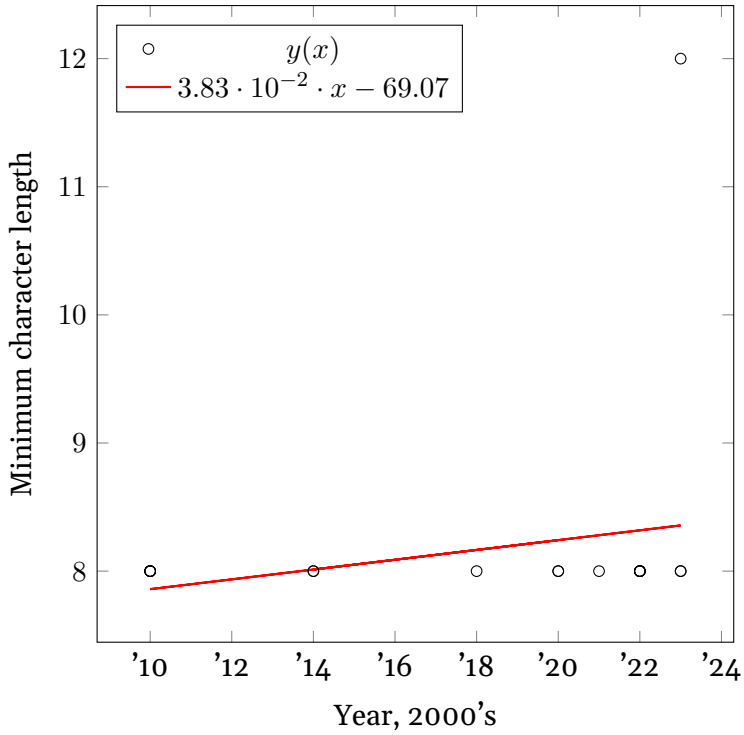

Figure 19: A scatter plot showing the revision date in contrast to password length for all of the policies with a date and length in dataset 1. (N = 20)

of Spearman was calculated to $P = 1.413 \cdot 10^{-9}$, allowing the null hypothesis to be rejected. According to Tukey's Fences, the combined datasets contained no outliers. The Pearson and Spearman correlation values are relatively close, which indicates a mostly linear relationship. See Figure 21.

6 Discussion

This section is dedicated to discussing the validity of this study, how the results presented in section 5 compare to the previous research presented in 2.5, as well as discussing what the results may entail in terms of their ethical and societal aspects.

6.1 Validity of Study

One of the validity concerns was not getting enough responses to be able to make generalized statements about the results. To make an argument regarding the validity of the study based on the number of responses, the collected data is presented in the context of random sampling, as a comparison can not be made in the context of a full population census. In the context of random sampling, comparing the number of responses to the size of the sample can produce a value that represents the error rate of the sample. In this case, the sample sizes consist of the 49 municipalities in Västra Götaland for dataset 1 and the rest of the 251 municipalities for dataset 2. A sample size of 22 out of 49 randomly selected municipalities for dataset 1 would have resulted in an error rate of 16% at a 95% confidence level. For dataset 2, the number would have been 112 out of 251, resulting in a margin of error of 7% at a 95% confidence level, with the combined dataset producing the same values. It would be inappropriate to argue that statistics

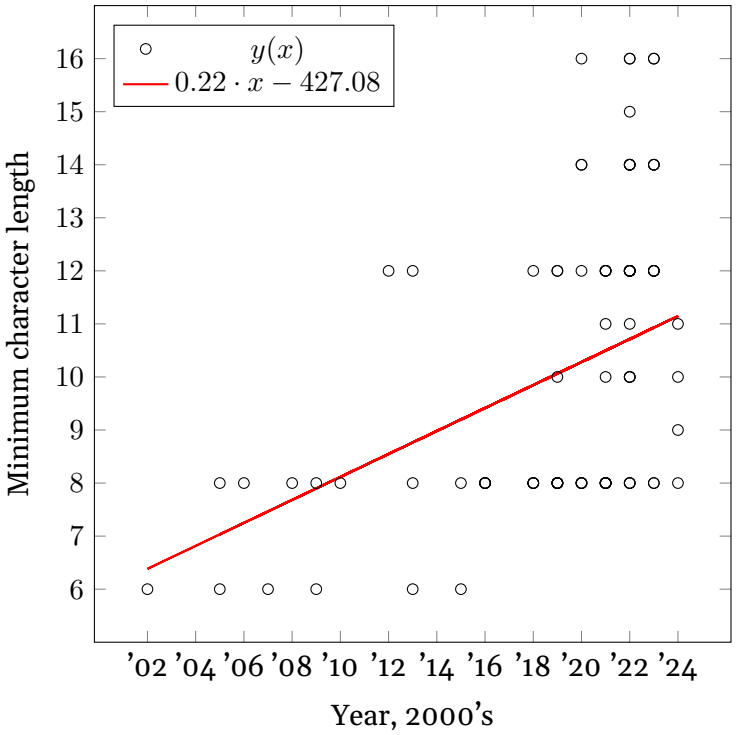

Figure 20: A scatter plot showing the revision date in contrast to password length for all policies with a date and length in dataset 2. (N = 92)

for the error rate and confidence level are valid as no sampling was used (Norris et al., 2019 as cited in Hatcher et al., 2020), however, an argument can still be made as to the response rates being high enough to be able to support the validity of the study. A 95% confidence level at a 7% margin of error is above the academic standard of 95% confidence at a 5% margin of error, but the numbers speak for some degree of representation based on the number of responses alone. It is worth iterating again that the numbers are not representative of the study as a whole or the values presented within, only an argument of the responses as they do not include factors such as volunteer bias. Too few historical documents were received to make generalized statements about research question 2.

Miscoding and the wrongful labeling of information have attempted to be avoided by the authors by creating a codebook with defined codes and then trying to apply the code book individually to all the policies. As presented in section 5.4, the Kappa was calculated between the two raters, and the pooled value was calculated to be $\kappa = 0.715$, a moderate level of agreement. As briefly mentioned within the section, the code "MFA /w password" had an extremely low level of agreement, even though the overall agreement rate was over 90%. Some of these differences in coding, for example, all the disagreements in the code "Minimum length", were due to missing information or statements, or simply reading the wrong data. Most of the differences were, however, due to an imprecise code book with definitions left open to interpretation. While re-coding those values that did not match between the raters, the codes were defined more thoroughly in their inclusion and exclusion criteria, and it is ultimately this version of the code book that is presented under section 5.2 and 5.3.

For reliability during translations, an independent third party vetted the translations of quotes and law texts. The original texts and their translations can be seen in appendix E. For the translation of names of organizations, these have either been taken from how the organizations themselves present on their international websites or taken from Hansson et al. (2024). The acronyms for the agencies have been written as presented in their original language.

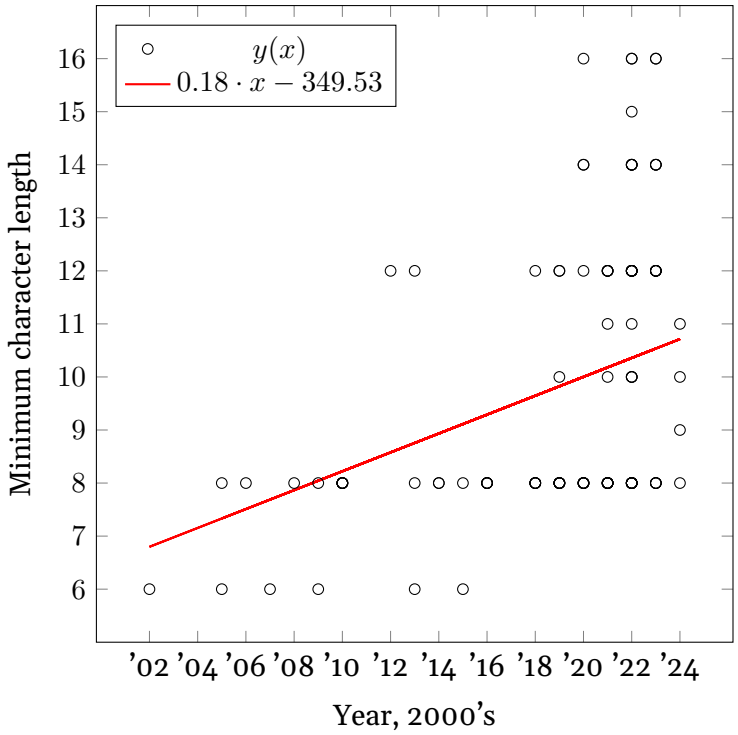

Figure 21: A scatter plot showing the revision date in contrast to password length for all policies with a date and length in the combined dataset. (N = 112)

The e-mail that was sent out had two revisions: one produced early that had not been vetted before it was sent out, and one that followed a published template that contained complementary information. While the response rates are similar – and the formulation of the e-mail should not have had a significant impact on the amount of data received – it was decided to split the data into two different datasets to guarantee that this did not influence the results. However, this renders dataset 1 tiny and makes most of its data unreliable and ultimately of little use by itself.

Some municipalities sent multiple current documents describing the same password policy, and it is worth noting that they sometimes contained contradictory information about the complexity requirement. One municipality stated in their password guidelines that four character classes were required, while it was stated in their handbook to workers that three out of four were required. Another municipality stated in one of their documents that two character classes were required, while another stated three out of four. In both of these examples, the three required character classes were chosen as the documents suggested that a Microsoft solution was in place. See section 2.4. All discrepancies were handled through a dialogue between the raters, and a judgment was made about what value was most likely to be in use based on the nature of the documents. For example, a user instruction with screenshots picturing the password creation process with the rules on-screen took precedence over a document stating the rules in free text, as it was deemed that the screenshots were a more reliable source. With the inconsistencies between two documents both stated as current, it was made clear that at least some policy documents were not written as a framework to implement but to document the currently used settings. The large number of municipalities that stated that they had no documents to give seems to support the hypothesis that the documents are made after the implementation. If this is the case, all data gathered has been an interpretation of an interpretation, partially mitigating the advantage of exactness that comes with the document analysis method, as presented in section 4.1. The drawbacks of document analysis as a data collection method include low retrievability

and documents lacking sufficient detail. This was noticeable throughout the entire gathering and analysis process, though an argument can be made that the response rates could have been worse without the legal requirement for a review over the retrieval process, as it would have been with a survey. Norris et al. (2021), for example, received a response rate of nearly 12%, and Gerlitz et al. (2021) received their 83 responses by being presented in a BSI newsletter. It is worth noting that even though this thesis had a larger reach than Gerlitz et al., the use of surveys instead of a document analysis would have produced uniform outputs. In a survey, there is meaning in not answering, but not writing a statement down in a document is much less of a deliberate act.

6.2 Relation to Previous Research

The following section goes into detail about how the results of this study compare to the ones presented in section 2.5. As this study is very similar to the one conducted by Gerlitz et al. (2021), their results are the primary source of comparison with the results of this study. The remaining articles being presented are similar in theming and have brought inspiration, but they differ too much in their aims and the variables they researched to make a comparison. However, the study by Sparrius et al. (2021) had a small impact on this study, and a minor comparison can be drawn. Sparrius et al. studied the ISPs of UK schools and noticed that 72% of them were overdue for an update as a consequence of a specified review date that had come to pass. A preconceived notion was formulated that Swedish municipalities would work with a similar system and that a comparison could be made. The truth was that very few of the retrieved policies contained an explicit review date, and as such, collected data regarding revision dates ended up not being analyzed. Although, curiously, two of the few policies that have a specified revision date and had their status of being currently in use confirmed were overdue for an update. See municipalities BV and BX in appendix B.3. This is far from the 72% that was observed within UK schools, but most other Swedish municipalities opted to specify that the policy was to be reviewed when the need arises instead of specifying a date.

As the organizations being studied by this study and by Gerlitz et al., both are based in Europe, and since Sweden and Germany both have somewhat similar cultures, it makes for an interesting comparison. Furthermore, the time frames of the studies are mere years apart, which makes this comparison relevant in terms of time. Additionally, the studies are very similar in their execution. The type of organization being examined differs between studies, however, as this one takes a look at municipalities, while Gerlitz et al. examines companies. It is also acknowledged that the Swedish public sector and private German organizations may have different legal requirements in place. As such, it is worth noting that the following comparison is made purely for the sake of discussion.

The study by Gerlitz et al., 2021 either does not examine or does not go into sufficient depth regarding login attempts before timeout, minimum changes, disallowing Unicode characters, the use of personal information, the use of MFA, and the act of writing down passwords, so these are not compared. Furthermore, dataset 1 is exempt from this comparison due to being too small for any meaningful conclusions to be drawn.

Minimum length: Organizations within both countries show a similar percentage of 95% of the policies having specified a minimum length requirement. However, a different spread of character lengths has been observed. The German companies have a higher amount of policies with a specified minimum length of eight at 52% compared to the 35.5% observed within

Swedish municipalities. Both countries have a generally low rate of policies specifying a minimum character length below eight characters, with German companies at 5% and Swedish municipalities at 1.8%. Swedish municipalities generally seem to have higher minimum character lengths, with 10.9% of policies specifying a minimum length of 9–11 characters (including the municipality with eight, 10, and 12 as its options), and 46.3% with 12 characters or more, compared to the German companies with 19% specifying 9–11 characters, and 19% with 12 or more characters minimum.

Complexity: Swedish municipalities and German companies showed somewhat similar rates of providing a specified complexity requirement, with 86.3% and 89% of policies specifying a complexity requirement, respectively. For Swedish municipalities, this includes the six municipalities (5.4%) with an undefined value. An approximate similarity was found between requiring the use of three of four character classes, with 50% of German companies and 55.4% of Swedish municipalities requiring it. 27% of German companies specified requiring the use of four character classes, while fewer Swedish municipalities required four at 19.1%. Of note is the fact that none of the observed German companies explicitly stated that no complexity requirements were in place, while two (1.8%) of Swedish municipalities specified that this requirement was not enforced, but this is most likely due to the larger number of responses of this thesis.

Password age: 70% of the observed German companies explicitly mentioned password expiry in their policies, which lines up with the 69% of Swedish municipalities that also include this particular requirement. For the Swedish municipalities, this includes the 13 municipalities (11.8%) with an undefined value. 90 days was observed as the most commonly used amount of days between password expiry in both countries, with 34% of German companies using this cycle rate and 23.6% of Swedish municipalities using it. A similar percentage of companies and municipalities explicitly stated the exclusion of a password expiry cycle at 3% of German companies and 3.6% of Swedish municipalities. 9.5% of German companies had a password expiry cycle below 90 days, and 30% had a cycle above 90 days. 2.7% of Swedish municipalities had a cycle rate below 90 days, and 30.9% (34 out of 110) above 90 days.

Password history: 47% of the observed German companies specified controlling newly created passwords against a list of previously used ones by a user, while 55.4% of Swedish municipalities explicitly state it and include the policies with an undefined value. The most prevalent number of passwords that can not be reused differs between the studies. A password history of 10 is the most common within German companies at 14.2%, while 24 is the most common in Sweden at 10.9%.

Blocklists: More German companies were observed to have implemented a blocklist compared to Swedish municipalities, at 41% and 25.45% of policies specifying the inclusion of a blocklist, respectively.

Compliance rate with NIST: The organizations used to rate policy compliance differ between this study and the one performed by Gerlitz et al., but NIST appears as a common denominator, and both use NIST's minimum length recommendation as the main measurement to gauge compliance. 89% of observed German companies achieve compliance with NIST based on minimum length, and 92.7% of Swedish municipalities achieve compliance. 5% of German companies directly go against this recommendation, while 1.8% of Swedish municipalities go against the recommended length.

6.3 Ethical and Societal Aspects

Since obtaining any of the information for this study is only possible as long as it is considered part of the public record–published online or not–and disclosing information from the public record is supported by law, we see no major ethical dilemma for releasing this information. In addition, publishing recommendations for password creation would, in theory, not reveal the actual password trends within Swedish municipalities. However, it is acknowledged that the results of this study can be used with malicious intent. If the results were to be interpreted as the municipalities in Sweden having poor information security routines due to their recommendations being considered "weak", there is a risk that the IT systems of these municipalities may be seen as attractive targets, which could lead to an increasing amount of attacks. However, the intent of the thesis is angled towards being a sort of wake-up call if such a result arises. To remedy the risk of singling out a specific municipality being seen as an attractive target for IT attacks, the names of the municipalities have been coded to maintain a level of anonymity within the collected data. However, total anonymity is not something that can be guaranteed due to the e-mails and replies sent to and from the municipalities being part of the public record. While it is not possible to connect a municipality to a municipality code without any outside information, municipalities that are within a local federation (Swedish kommunalförbund) could be singled out by counting municipalities that share the same policy. It is expected that the municipalities were aware of this fact during the initial examination when deciding whether or not it was appropriate to send the requested policies.

6.4 Benefits

The Critical Entities Resilience Directive was enacted by the European Union in 2022 to strengthen the security of essential services, like public administration, to disasters, both physical and digital (Council of European Union, 2022). In this directive, governments are required to make risk assessments and plan for eventual scenarios accordingly. This study could be used as a part of that risk assessment. The results of this study can arguably benefit target 16.6 of the UN sustainability goals: Develop effective, accountable, and transparent institutions at all levels. Having a strong password creation strategy is merely one of the steps towards having a proper cyber security strategy. This, in turn, leads to the reduced risk of being affected by cyber attacks. Less cyber attacks means reduced downtime and saved resources in the shape of both time and money that can be spent on something else, thus having a positive effect on effectiveness. If this report ends up having a positive influence on any municipality's cyber security efforts, the authors see this as a step towards reaching the aforementioned sustainability goal.

6.5 General Discussion

In section 4.1, availability is presented as an advantage of the document research method. However, it was eventually discovered that the nature of the study essentially nullifies the availability advantage. A majority of Swedish municipalities were not too keen to publish their password guidelines on their websites, with a mere 34 out of the 290 municipalities (11.7%) having their password policies published.

It was somewhat concerning to observe such many policies including a forced password change requirement. As stated in the report published by the IIS, this practice is hard to kill off, and this became evident after the data analysis (Löwinder, 2016). Both NIST and the IIS bring up the fact that the practice of forced password changes brings more harm than good, as it often

leads to poor password creation habits (Löwinder, 2016; NIST, 2022). It is strongly urged that the Swedish municipalities consider whether this practice truly is worth keeping going forward.

In section 2.2.3, it is mentioned that previous research points towards that long passwords without complexity requirements generally lead to passwords that are harder to crack, in addition to providing higher levels of user-friendliness. However, it was observed that a significant amount of municipalities utilize a minimum composition of comp8. Comp8 is defined as having a minimum of eight characters and a complexity requirement of three classes. A length of eight is on the low end, and according to P. Grassi et al. (2017), the complexity requirements are often detrimental to users' ability to create unpredictable passwords. A total of 56 out of the 131 municipalities (42.7%) analyzed utilize comp8 as their password composition standard. As Tan et al. (2020) suggests, it might be better to phase out complexity requirements in favor of higher length requirements in combination with blocklists and password strength checks during password creation. It is worth iterating that ENISA states that passwords as short as nine can be cracked in a manner of seconds. The 44% of the municipalities that are within this category are encouraged to reevaluate if their current password policy is sufficiently strong for their security needs.

With MSB being an important part of the municipalities' civil defense, it is curious that they have not published recommendations that are more concrete. While no password policy will fit all environments, the agency could create a more defined minimum level of security that organizations should adhere to in order to raise the security among those who are the most vulnerable.

With the NIS2-directive being formulated as law (SOU 2024:18) and to be enacted on January the 1st, 2025, Swedish organizations need to inspect their digital infrastructure and make a judgment if it is robust enough to follow the new standards. While multi-factor authentication is recommended by nearly every organization, the use of passwords as a single authentication method is still high due to either the systems not supporting other authentication methods or MFA being simply an alternative instead of a requirement. The same study could be conducted in a year or two to see if the enactment of this law has had an impact on the use of multi-factor authentication or password length. Some municipalities were observed to have already transitioned, or are in the middle of transitioning towards a completely passwordless authentication solution. As such, another future study could be to track how many municipalities have transitioned since this study was performed, or document the hindrances municipalities face during the transition.

7 Conclusions

This study attempted to document the current state of password policies within municipalities in Sweden. As volunteer bias was a concern, see section 4.4, presenting the study's validity as a value would be impossible. However, if the study had contained no bias, the response rates acquired would have achieved a 7% margin of error at a 95% confidence level for both dataset 2 and the combined dataset. While being above the industry standard of 5% margin of error at a 95% confidence level, an argument can be made that the study still holds some level of confidence. The study aimed to answer three questions: What is the compliance rate for municipalities' password policies compared to published recommendations? What is the age of a municipality's current policy, and how long did they use the last one? Is there a relationship between the date of the policy and its required minimum length? While the first and the third research questions were answered with some degree of representation, not enough samples were provided for older documents to represent reality accurately. The compliance rates for dataset 2 against the

NIST recommendations were 92.7%, which aligns with previous research. The compliance rates for dataset 2 against the 24 bits of entropy required by SUNET to reach assurance level 1 for their user verification system were 91.8%. The recommendations from the other organizations were vague enough to leave much room for interpretation of what they saw as secure. The strictest recommendations came from ENISA, which insinuated a recommended character length of 15 and a complexity of two. This recommendation was only achieved by a single municipality. For research question three, the relationship between the age of the policy and the minimum length requirement was large and mostly linear within the retrieved data, which can be stated with a very high degree of confidence.

Even if passwords are not the most secure authentication method, it seems to be hard to forego using them altogether. The authors believe it will be an alternative as an authentication method for most municipalities for a while longer, even if municipalities have begun implementing MFA and some have gone passwordless. While in this transition period, it is important to recognize the weaknesses of the current method and try to alleviate them, and not only look into the future.

References

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). *Thesis projects*. Springer London. ISBN: 9781848000094. https://doi.org/10.1007/978-1-84800-009-4

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/qrj0902027

Braun, V., & Clarke, V. (2013). *Successful qualitative research: A practical guide for beginners*. SAGE Publications. ISBN: 9781847875822.

Burr, W., Dodson, D., Newton, E., Perlner, R., Polk, T., Gupta, S., & Nabbus, E. (2013, August). Electronic authentication guideline. *NIST*. https://doi.org/10.6028/NIST.SP.800-63-2

Campbell, J. L., Quincy, C., Osserman, J., & Pedersen, O. K. (2013). Coding in-depth semistructured interviews: Problems of unitization and intercoder reliability and agreement. *Sociological Methods & Research*, *42*(3), 294–320. https://doi.org/10.1177/0049124113500475

Citrix. (2024, February). Customize security and privacy policies. https://docs.citrix.com/en-us/citrix-workspace/experience/policies.html

Cohen, J. (1977). Chapter 9 - f tests of variance proportions in multiple regression/correlation analysis. In J. Cohen (Ed.), *Statistical power analysis for the behavioral sciences* (pp. 413–414). Academic Press. ISBN: 978-0-12-179060-8. https://doi.org/10.1016/B978-0-12-179060-8.50014-1

Council of European Union. (2022). Directive (EU) no 2022/2557. http://data.europa.eu/eli/dir/2022/2557/oj

de Winter, J., Gosling, S., & Potter, J. (2016). Comparing the Pearson and Spearman correlation coefficients across distributions and sample sizes: A tutorial using simulations and empirical data. *Psychological Methods*, *21*, 273–290. https://doi.org/10.1037/met0000079

Denning, D. (1982). *Cryptography and data security*. Addison-Wesley Longman Publishing Co., Inc. ISBN: 0201101505.

Egelman, S., Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., & Cranor, L. Of passwords and people: Measuring the effect of password-composition policies. en. In: CHI '11: Proceedings of the SIGCHI conference on Human Factors in Computing Systems, Vancouver, -1, 2011, May. https://doi.org/10.1145/1978942.1979321

ENISA. *Cybersecurity guide for smes - 12 steps to securing your business*. 2021, June. https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

ENISA. (2022, November). Authentication methods. https://www.enisa.europa.eu/topics/incident-response/glossary/authentication-methods

ENISA. (2024, April). About enisa - the european union agency for cybersecurity. https://www.enisa.europa.eu/about-enisa

Gerlitz, E., Haering, M., Smith, M., & Tiefenau, C. (2023). Evolution of password expiry in companies: Measuring the adoption of recommendations by the german federal office for information security [19th Symposium on Usable Privacy and Security (SOUPS), Anaheim, CA, AUG 07-08, 2023]. *Proceedings of the nineteenth symposium on the usable privacy and security, SOUPS 2023*, 191–210. ISBN: 978-1-939133-36-6.

Gerlitz, E., Häring, M., & Smith, M. (2021). Please do not use !?_ or your license plate number: Analyzing password policies in german companies. *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 17–36. ISBN: 978-1-939133-25-0. https://www.usenix.org/conference/soups2021/presentation/gerlitz

Google. (n.d.-a). Create a strong password & a more secure account. https://support.google.com/accounts/answer/32040?#zippy=%2Cmake-your-password-longer-more-memorable

Google. (n.d.-b). Enforce and monitor password requirements for users. https://support.google.com/a/answer/139399?hl=en

Gosset, W. S. (1908). The probable error of a mean [Originally published under the pseudonym "Student".]. *Biometrika*, *6*(1), 1–25. https://seismo.berkeley.edu/~kirchner/eps_120/Odds_n_ends/Students_original_paper.pdf

Grassi, P., Newton, E., Fenton, J., Perlner, R., Regenscheid, A., Burr, W., Richer, J., Lefkovitz, N., Danker, J., Choong, Y.-Y., Greene, K., & Theofanos, M. (2017, June). Nist sp 800-63b digital identity guidelines. https://doi.org/10.6028/NIST.SP.800-63b

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017, June). *Digital identity guidelines: Revision 3*. https://doi.org/10.6028/nist.sp.800-63-3

Hall, J., Larson, T., Buck, A., Flores, J., Sherer, T., Lyon, R., Lamos, B., Borsecnik, J., luc-msft, Takata, J., Foulds, I., Torble, T., Martinez, J., MonikaReddy-MSFT, Turscak, M., Love, C., Sharma, S., MSshujia, yishengjin1413, … Ross, E. (2024, April). https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy

Hansson, G., van Dorrestein, M., Dahlqvist, N., Norbergh, E., Eriksson, B., Heikkilä, R., Larsson, T., Kirchmeyer, N., Malmgren, R., Oliver, A., & Wollberg, B. *Utrikes namnbok*. 2024.

Hatcher, W., Meares, W. L., & Heslen, J. (2020). The cybersecurity of municipalities in the united states: An exploratory survey of policies and practices. *Journal of Cyber Policy*, *5*(2), 302–325. https://doi.org/10.1080/23738871.2020.1792956

Hendarto, I. L. S., & Kurniawan, Y. (2017). Performance factors of a cuda gpu parallel program: A case study on a pdf password cracking brute-force algorithm. *2017 International Conference on Computer, Control, Informatics and its Applications (IC3INA)*, 35–40. https://doi.org/10.1109/IC3INA.2017.8251736

IEEE IRDS. (2023). International roadmap for deviecs and systems 2023 update. https://irds.ieee.org/images/files/pdf/2023/2023IRDS_BC.pdf

Indeed Editorial Team. (2023, July). What is a data collection letter? (with template and example). *Indeed*. https://www.indeed.com/career-advice/career-development/data-collection-letter-sample

Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., & Lopez, J. (2012). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. *2012 IEEE Symposium on Security and Privacy*, 523–537. https://doi.org/10.1109/SP.2012.38

Keszthelyi, A. (2013). About passwords. *Acta Polytechnica Hungarica*, *10*, 99–118. https://www.researchgate.net/publication/293518235_About_Passwords

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., & Egelman, S. (2011). Of passwords and people: Measuring the effect of password-composition policies. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2595–2604. ISBN: 9781450302289. https://doi.org/10.1145/1978942.1979321

Lindner, J. (2024, February). Statistics about the average word length. https://gitnux.org/average-word-length/

Löwinder, A.-M. E. (2016, September). Lösenord för alla. *Internetstiftelsen*. https://internetstiftelsen.se/kunskap/rapporter-och-guider/losenord-for-alla/

McHugh, M. (2012). Interrater reliability: The kappa statistic. *Biochemia medica : časopis Hrvatskoga društva medicinskih biokemičara / HDMB*, 22, 276–82. https://doi.org/10.11613/BM.2012.031

Microsoft. (2021, July). Minimum password length auditing and enforcement on certain versions of windows. https://support.microsoft.com/en-us/topic/minimum-password-length-auditing-and-enforcement-on-certain-versions-of-windows-5ef7fecf-3325-f56b-cc10-4fd565aacc59

Morgan, H. (2022). Conducting a qualitative document analysis. *The Qualitative Report*, *27(1)*, 64–77. https://doi.org/10.46743/2160-3715/2022.5044

MSB. (2024a, January). Säkra dina lösenord. https://www.msb.se/sv/rad-till-privatpersoner/informationssakerhet/sakra-dina-losenord/
MSB. (2024b, March). Vårt uppdrag. https://www.msb.se/sv/om-msb/vart-uppdrag/
NIST. (2022, March). Nist special publication 800-63: Digital identity guidelines frequently asked questions. https://pages.nist.gov/800-63-FAQ/
Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2021). Managing cybersecurity at the grass-roots: Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*, *43*(8), 1173–1195. https://doi.org/10.1080/07352166.2020.1727295
Okta. (n.d.-a). About us. https://www.okta.com/company/
Okta. (n.d.-b). *Configure a password policy*. https://help.okta.com/en-us/content/topics/security/policies/configure-password-policies.htm
Okta. (n.d.-c). Password policies. https://help.okta.com/en-us/content/topics/security/policies/about-password-policies.htm
Palko, M. (2023, October). The evolution of windows authentication. https://techcommunity.microsoft.com/t5/windows-it-pro-blog/the-evolution-of-windows-authentication/bap/3926848
Pamnani, V. (2017). Password policy. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/password-policy
Proctor, R. W., Lien, M.-C., Vu, K.-P. L., Schultz, E. E., & Salvendy, G. (2002). Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, Instruments, & Computers*, *34*(2), 163–169. https://doi.org/10.3758/bf03195438
Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4). https://doi.org/10.3390/fi11040089
Shay, R., Komanduri, S., Durity, A. L., Huh, S., Mazurek, M. L., Segreti, S. M., Ur, B., Bauer, L., Christin, N., & Cranor, L. F. (2016). Designing password policies for strength and usability. *ACM Trans. Inf. Syst. Secur.*, *18*(4). https://doi.org/10.1145/2891411
Sherif, A. (2024). Global market share held by computer operating systems 2012-2024, by month. https://www.statista.com/statistics/268237/global-market-share-held-by-operating-systems-since-2009/#statisticContainer
Sparrius, M., Sadok, M., & Bednar, P. (2021). What can we learn from the analysis of information security policies? the case of uk's schools. In S. Furnell & N. Clarke (Eds.), *Human aspects of information security and assurance* (pp. 81–90). Springer International Publishing. ISBN: 978-3-030-81111-2.
SUNET. (n.d.). Om sunet. https://www.sunet.se/om-sunet
SUNET. (2020a, June). Swamid identity assurance level 1 profile. https://wiki.sunet.se/download/attachments/78218822/SWAMID%20Identity%20Assurance%20Level%201%20Profile%20v3.0%20FINAL.pdf?version=1%5C&modificationDate=1592295959000%5C&api=v2
SUNET. (2020b, June). Swamid identity assurance level 2 profile. https://wiki.sunet.se/download/attachments/78218828/SWAMID%20Identity%20Assurance%20Level%202%20Profile%20v2.0%20FINAL.pdf?version=1%5C&modificationDate=1592296093000%5C&api=v
SUNET. (2020c, June). Swamid identity assurance level 3 profile. https://wiki.sunet.se/download/attachments/83494432/SWAMID%20Identity%20Assurance%20Level%203%20Profile%20v1.0%20FINAL.pdf?version=1%5C&modificationDate=1592296769000%5C&api=v2
Swedish Freedom of the Press Act, SFS 1949:105. (2022). Justitiedepartementet L6. https://lagen.nu/1949:105

Tan, J., Bauer, L., Christin, N., & Cranor, L. F. (2020). Practical recommendations for stronger, more usable passwords combining minimum-strength, minimum-length, and blocklist requirements. *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 1407–1426. ISBN: 9781450370899. https://doi.org/10.1145/3372297.3417882

Temoshok, D., Proud-Madruga, D., Choong, Y.-Y., Galluzzo, R., Gupta, S., LaSalle, C., Lefkovitz, N., & Regenscheid, A. (2022a, December). *Digital identity guidelines*. https://doi.org/10.6028/nist.sp.800-63-4.ipd

Temoshok, D., Proud-Madruga, D., Choong, Y.-Y., Galluzzo, R., Gupta, S., LaSalle, C., Lefkovitz, N., & Regenscheid, A. (2022b, December). Nist sp 800-63-4 digital identity guidelines. *NIST*. https://doi.org/10.6028/NIST.SP.800-63-4.ipd

The Public Access to Information and Secrecy Act, SFS 2009:400. (2024). Justitiedepartementet L6. https://lagen.nu/2009:400

the Security Factory. (2020, May). Password cracking speed. https://thesecurityfactory.be/password-cracking-speed/

Vries, H. D., Elliott, M. N., Kanouse, D. E., & Teleki, S. S. (2008). Using pooled kappa to summarize interrater agreement across many items. *Field Methods*, *20*(3), 272–282. https://doi.org/10.1177/1525822X08317166

Wåhlén, M., Fahlström, P., Näslund, A., Olsson, D., Hesselberg, D., Ström, J., Bergstedt, L., Jaurén, D., Hultgren, M., & Murray, M. (2024, February). Threat intelligence report 2024. *Truesec*.

Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. *Proceedings of the 17th ACM Conference on Computer and Communications Security*, 162–175. ISBN: 9781450302456. https://doi.org/10.1145/1866307.1866327

Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password – a laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies*, *133*, 26–44. https://doi.org/10.1016/j.ijhcs.2019.08.006

A Email templates

A.1 Template used for dataset 1

Subject: **Begäran av allmänna handlingar - Exjobb om lösenordssäkerhet**
Hej,

Vi är två studenter på Högskolan i Skövde som skriver ett examensarbete för programmet Nätverk och Systemadministration om kommuners lösenord och lösenordspolicys. Vi skulle vilja begära ut de interna document som stryker riktlinjer för lösenord och lösenordsrutiner för kommunens anställdas personalkonton. Vi skulle vilja ha både det nuvarande regelverket, samt en version bakåt (2 versioner totalt). Vi anser att detta är i enlighet med offentlighets- och sekretesslagen (2009:400) kapitel 6 då informationens avslöjande antingen har en smärre, eller ingen som helst påverkan på kommunens säkerhet. Vi hittade ingenting på er hemsida och/eller i ert diarium online så vi skulle uppskatta om ni kunde hjälpa oss att antingen hitta informationen eller vägleda dit vi ska.
Tack för er samverkan.

Ha en fortsatt trevlig vecka,
Filip Olsson och David Halén

A.2 Edited template, nothing published online

Subject: **Begäran av allmänna handlingar - Exjobb om lösenordssäkerhet**
Hej,

Vi är två studenter på Högskolan i Skövde som skriver ett examensarbete för programmet Nätverk och Systemadministration om kommuners lösenord och lösenordspolicys. Syftet med arbetet är att jämföra samtliga kommuners lösenords-riktlinjer eller policys mot de rekommendationer som organisationer såsom MSB, NIST, Internetstiftelsen, m.fl. publicerar. Vi vill sen jämföra era nuvarande riktlinjer mot en tidigare revision för att få en bild av hur ofta man kan förvänta sig att dessa revideras, och vilka förändringar som sker för att upprätthålla en bra standard. Med tanke på att hotbilden inom IT-säkerheten ständigt växer så vill vi göra en så kallad “current state analysis” för att se om kommunerna tar initiativet att utveckla sin säkerhet i samband med att hoten utvecklas.
Vi skulle vilja begära ut de dokument som beskriver riktlinjer för lösenord och lösenordsrutiner för kommunens personalkonton. Vi skulle vilja ha både det nuvarande regelverket, samt en version bakåt (två versioner totalt). Vi anser att detta är i enlighet med offentlighets- och sekretesslagen (2009:400) kapitel 6 då informationens avslöjande antingen har en mindre eller ingen påverkan på kommunens säkerhet. Vi hittade ingenting bland er författningssamling och/eller styrdokument online så vi skulle uppskatta om ni kunde hjälpa oss att antingen hitta informationen eller vägleda dit vi ska. Informationen kommer att publiceras men det kommer inte kunna härledas tillbaka till en specifik kommun då vi kommer att implementera en form av kodning i den insamlade datan.
Vill ni verifiera vår status som studenter på Högskolan i Skövde, eller validiteten av exjobbet så kan ni kontakta vår handledare enligt uppgifter nedan.
Tack för er samverkan.

Ha en fortsatt trevlig vecka,
Filip Olsson och David Halén

Handledare på Högskolan i Skövde:
Johan Zaxmy:
+46 XX XXX XX XX
[redacted]

Studenter:
Filip Olsson:
+46 XX XXX XX XX
[redacted]

David Halén:
+46 XX XXX XX XX
[redacted]

A.3 Edited template, when documents published online

Subject: **Begäran av allmänna handlingar - Exjobb om lösenordssäkerhet**
Hej,

Vi är två studenter på Högskolan i Skövde som skriver ett examensarbete för programmet Nätverk och Systemadministration om kommuners lösenord och lösenordspolicys. Syftet med arbetet är att jämföra samtliga kommuners lösenords-riktlinjer eller policys mot de rekommendationer som organisationer såsom MSB, NIST, Internetstiftelsen, m.fl. publicerar. Vi vill sen jämföra era nuvarande riktlinjer mot en tidigare revision för att få en bild av hur ofta man kan förvänta sig att dessa revideras, och vilka förändringar som sker för att upprätthålla en bra standard. Med tanke på att hotbilden inom IT-säkerheten ständigt växer så vill vi göra en så kallad "current state analysis" för att se om kommunerna tar initiativet att utveckla sin säkerhet i samband med att hoten utvecklas.
Vi skulle vilja begära ut de dokument som beskriver riktlinjer för lösenord och lösenordsrutiner för kommunens personalkonton. Vi hittade en version genom er hemsida, och vi skulle vilja veta ifall den är aktuell i dagsläget; {LINK} Utöver det skulle vi vilja få en äldre version av dokumentet, om ni har en. Vi anser att detta är i enlighet med offentlighets- och sekretesslagen (2009:400) kapitel 6 då informationens avslöjande antingen har en mindre eller ingen påverkan på kommunens säkerhet. Informationen kommer att publiceras men det kommer inte kunna härledas tillbaka till en specifik kommun då vi kommer att implementera en form av kodning i den insamlade datan.
Vill ni verifiera vår status som studenter på Högskolan i Skövde, eller validiteten av exjobbet så kan ni kontakta vår handledare enligt uppgifter nedan.
Tack för er samverkan.

Ha en fortsatt trevlig vecka,
Filip Olsson och David Halén

Handledare på Högskolan i Skövde:
Johan Zaxmy:
+46 XX XXX XX XX
[redacted]

Studenter:
Filip Olsson:
+46 XX XXX XX XX
[redacted]

David Halén:
+46 XX XXX XX XX
[redacted]

A.4 Template used when no response given after three weeks

Subject: **Begäran av allmänna handlingar - Exjobb om lösenordssäkerhet**
Hej,

Vi mailade er för ca 3 veckor sen och har fortfarande inte fått ett svar, så vi tänkte göra ett till försök.

Vi är två studenter på Högskolan i Skövde som skriver ett examensarbete för programmet Nätverk och Systemadministration om kommuners lösenord och lösenordspolicys. Syftet med arbetet är att jämföra samtliga kommuners lösenords-riktlinjer eller policys mot de rekommendationer som organisationer såsom MSB, NIST, Internetstiftelsen, m.fl. publicerar. Vi vill sen jämföra era nuvarande riktlinjer mot en tidigare revision för att få en bild av hur ofta man kan förvänta sig att dessa revideras, och vilka förändringar som sker för att upprätthålla en bra standard. Med tanke på att hotbilden inom IT-säkerheten ständigt växer så vill vi göra en så kallad "current state analysis" för att se om kommunerna tar initiativet att utveckla sin säkerhet i samband med att hoten utvecklas.
Vi skulle vilja begära ut de dokument som beskriver riktlinjer för lösenord och lösenordsrutiner för kommunens personalkonton. Vi skulle vilja ha både det nuvarande regelverket, samt en version bakåt (två versioner totalt). Vi anser att detta är i enlighet med offentlighets- och sekretesslagen (2009:400) kapitel 6 då informationens avslöjande antingen har en mindre eller ingen påverkan på kommunens säkerhet. Vi hittade ingenting bland er författningssamling och/eller styrdokument online så vi skulle uppskatta om ni kunde hjälpa oss att antingen hitta informationen eller vägleda dit vi ska. Informationen kommer att publiceras men det kommer inte kunna härledas tillbaka till en specifik kommun då vi kommer att implementera en form av kodning i den insamlade datan.
Vill ni verifiera vår status som studenter på Högskolan i Skövde, eller validiteten av exjobbet så kan ni kontakta vår handledare enligt uppgifter nedan.
Tack för er samverkan.

Ha en fortsatt trevlig vecka,
Filip Olsson och David Halén

Handledare på Högskolan i Skövde:
Johan Zaxmy:
+46 XX XXX XX XX
[redacted]

Studenter:
Filip Olsson:

+46 XX XXX XX XX
[redacted]

David Halén:
+46 XX XXX XX XX
[redacted]

B Datasets

B.1 Dataset 1

Code	Passwordless	No policy	Rejected	Min Length	Char classes	Login attempts	Password cycle	Password history	Minimum changes
01	☐	☐	☐						
02	☐	☐	☑	8.00	3.00				
03	☐	☐	☐	12.00		5	180	6	
04	☐	☐	☐	8.00	3.00		Undefined		
05	☐	☑	☐	12.00	2.00				
06	☐	☐	☐	8.00	3.00	10	180-270	24	1*
07	☐	☐	☐	8.00	3.00	5	90	Undefined	
08	☐	☐	☐	8.00	3.00				
09	☐	☑	☐	8.00	3.00				
10	☐	☐	☐	8.00	3.00	10	180-270	24	1*
11	☐	☐	☐		3.00				
12	☐	☐	☐	8.00	3.00	10	180-270	24	1*
13	☐	☐	☐	8.00	3.00		60	Undefined	
14	☐	☐	☐	12.00			Undefined		
15	☐	☐	☐	8.00	3.00	10	180-270	24	1*
16	☐	☐	☐	8.00	3.00	3	90	Undefined	Undefined
17	☐	☐	☐	8.00	3.00	5	120	8	
18	☑	☐	☐	X	X	X	X	X	X
19	☐	☐	☐	8.00	3.00	10	180-270	24	1*
20	☐	☐	☐	8.00	3.00	10	180-270	24	1*
21	☐	☑	☐	8.00	3.00			24	
22	☐	☑	☐	8.00		10	90	24	

Code	Dissallow Unicode-characters	No personal info	No sequences or patterns	Blacklist/No dictionary words	MFA w/ password
01	☐	☑	☐	☑	☐
02	☑	☑	☐	☐	☐
03	☑	☐	☐	☐	☐
04	☑	☑	☐	☐	☐
05	☐	☑	☐	☐	☑
06	☑	☑	☑	☑	☐
07	☑	☐	☐	☐	☐
08	☑	☑	☐	☐	☐
09	☑	☑	☑	☐	☐
10	☑	☑	☑	☑	☐
11	☑	☑	☐	☐	☐
12	☑	☑	☑	☑	☐
13	☐	☑	☐	☐	☐
14	☐	☐	☐	☐	☐
15	☑	☑	☑	☑	☐
16	☑	☑	☐	☐	☐
17	☑	☑	☑	☐	☐
18	☐	☐	☐	☐	☐
19	☑	☑	☑	☑	☐
20	☑	☑	☑	☑	☐
21	☑	☑	☐	☐	☐
22	☐	☑	☑	☐	☐

Code	Safe to write down	Enacted	Valid through
01	No	2023	
02	No	2023	
03	No		
04	No		
05			
06		2022	
07	No	2021	
08	No	2023	
09	No		
10		2022	
11	Safe	2023	Until further notice
12	No	2022	
13		2020	
14		2023	2026-12-31
15	No	2022	
16		2014	
17	Safe	2018	
18			
19		2022	
20		2022	
21	No		
22			

B.2 Dataset 1 old

Code	Min Length	Char classes	Login attempts	Password cycle	Password history	Minimum changes	Dissallow Unicode-characters
06	8.00	3.00	3	60			☐
10	8.00	3.00	3	60			☐
11	8.00	2.00	6	90			☐
12	8.00	3.00	3	60			☐
15	8.00	3.00	3	60			☐
18	8.00	4.00		90			☐
19	8.00	3.00	3	60			☐
20	8.00	3.00	3	60			☐

Code	No personal info	No sequences or patterns	Blacklist/No dictionary words	MFA w/ password	Safe to write down	Enacted
06	☐	☐	☐	☐		2010
10	☐	☐	☐	☐		2010
11	☐	☐	☐	☐	Safe	2020
12	☐	☐	☐	☐	Safe	2014
15	☐	☐	☐	☐		2010
18	☐	☐	☐	☐		
19	☐	☐	☐	☐		2010
20	☐	☐	☐	☐		2010

Code	Valid through
06	
10	
11	
12	
15	
18	
19	
20	

B.3 Dataset 2

Code	Passwordless	No policy document	Rejected	Förbund/Delar	Min Length	Char classes	Login attempts	Password cycle	Password history
AA	☐	☐	☐	☑	8.00	Undefined		90	24
AB	☐	☐	☐	☐	8.00	2.00	5	Undefined	
AC	☐	☐	☐	☐	11.00	3.00		90	
AD	☐	☐	☐	☑	12.00	3.00	5	365	
AE	☐	☐	☐	☑	12.00	3.00			
AF	☐	☐	☐	☐	8.00	4.00		90	Undefined
AG	☐	☐	☐	☐	8.00	3.00		90	Undefined
AH	☐	☐	☐	☐	12.00		5	90	
AI	☐	☑	☐	☐	10.00	3.00			
AJ	☐	☐	☐	☐	12.00	3.00		360	
AK	☐	☐	☐	☑	8.00	Undefined		90	24
AL	☐	☐	☐	☐	15.00	3.00			
AM	☐	☐	☐	☑	12.00	3.00	5	365	
AN	☐	☐	☐	☐		4.00			
AO	☐	☐	☐	☐		4.00			Undefined
AP	☐	☐	☐	☐	12.00				
AQ	☐	☐	☐	☐	16.00	No		No	
AR	☐	☑	☐	☐	15.00	No		365	24
AS	☐	☐	☐	☐	14.00	2.00		730	
AT	☐	☐	☐	☑	8.00	3.00	3		90 Undefined
AU	☐	☐	☐	☐	8.00	3.00		365	
AV	☐	☐	☐	☑	12.00	3.00	5	365	
AW	☐	☐	☐	☐	14.00	3.00	5	365	10
AX	☐	☐	☐	☐	8.00	3.00		Undefined	Undefined
AY	☐	☑	☐	☐	12.00	2.00		90	24
AZ	☐	☐	☐	☑	8.00	Undefined		90	24
BA	☐	☐	☐	☐	8.00	3.00		Undefined	Undefined
BB	☐	☑	☐	☐	8.00	3.00			24
BC	☐	☐	☐	☐	6.00	4.00		45	Undefined

Code	Minimum changes	Dissallow Unicode-characters	No personal info	No sequences or patterns	Blacklist/No dictionary words
AA		☐	☐	☐	☐
AB		☐	☑	☑	☑
AC		☐	☐	☐	☐
AD		☑	☑	☑	☑
AE		☐	☑	☑	☐
AF		☑	☑	☐	☑
AG		☑	☑	☐	☐
AH		☑	☐	☐	☐
AI		☐	☐	☐	☐
AJ		☐	☑	☐	☐
AK		☐	☐	☐	☐
AL		☐	☐	☐	☐
AM		☑	☑	☑	☑
AN		☐	☑	☐	☐
AO		☐	☑	☐	☐
AP		☐	☑	☑	☑
AQ		☐	☐	☐	☐
AR		☐	☐	☑	☐
AS		☐	☐	☐	☐
AT		☐	☐	☐	☐
AU		☐	☑	☑	☑
AV		☑	☑	☑	☑
AW	1*	☑	☑	☐	☐
AX		☐	☐	☐	☐
AY		☐	☐	☐	☐
AZ		☐	☐	☐	☐
BA		☑	☐	☐	☐
BB		☐	☑	☐	☐
BC		☐	☑	☐	☑

Code	MFA w/ password	Safe to write down	Enacted	Valid through
AA	☐			
AB	☐		2021	
AC	☐	Safe	2024	
AD	☐		2022	
AE	☐	Safe		
AF	☐		2023	
AG	☐		2018	
AH	☐		2013	
AI	☐			
AJ	☐			
AK	☐			
AL	☐	Safe		
AM	☐		2022	
AN	☐	Safe	2021	Until further notice
AO	☐	Safe	2023	
AP	☐	Safe		2025-04-01
AQ	☐		2020	
AR	☐		2022	
AS	☐		2023	
AT	☐		2016	
AU	☐	Safe	2022	
AV	☐		2022	
AW	☐	Safe	2023	Every 4th year
AX	☐			
AY	☐			
AZ	☐			
BA	☐		2020	Every 4th year
BB	☐			
BC	☐		2015	

Code	Passwordless	No policy document	Rejected	Förbund/Delar	Min Length	Char classes	Login attempts	Password cycle	Password history
BD	☐	☐	☐	☐	14.00	4.00			
BE	☐	☐	☐	☑	8.00	3.00	3	90	Undefined
BF	☐	☑	☐	☐	17.00				
BG	☐	☐	☐	☑	8.00	4.00	Undefined	Undefined	Undefined
BH	☐	☐	☐	☑	8.00	3.00	3	90	Undefined
BI	☐	☑	☐	☐	14.00	4.00		120	Undefined
BJ	☐	☐	☐	☐	15.00	3.00			Undefined
BK	☐	☑	☐	☐	12.00	3.00			Undefined
BL	☐	☑	☐	☐	9.00	3.00		180	10
BM	☐	☑	☐	☐	8.00	4.00			
BN	☐	☐	☐	☐	14.00	3.00		180	6
BO	☐	☐	☐	☐	8.00	3.00		90	Undefined
BP	☐	☐	☐	☐	12.00	3.00	5		
BQ	☐	☑	☐	☐	8.00	3.00		90	
BR	☐	☑	☐	☐	12.00			365	
BS	☐	☐	☐	☐	8.00		Undefined	Undefined	Undefined
BT	☐	☐	☐	☐	12.00	2.00		90	30 / 1 year
BU	☐	☐	☐	☐	8.00	3.00		180	
BV	☐	☐	☐	☐	8.00	4.00		90	
BW	☐	☐	☐	☐	12.00	4.00		Undefined	
BX	☐	☐	☐	☐					
BY	☐	☐	☐	☐	8.00	4.00		90	Undefined
BZ	☐	☐	☐	☐	8.00	3.00		Undefined	
CA	☐	☐	☐	☐	8.00	3.00		180	Undefined
CB	☐	☐	☐	☐	14.00	4.00	5		
CC	☐	☐	☐	☑	12.00	3.00			
CD	☐	☐	☐	☑	16.00		12	No	12
CE	☑	☐	☐	☐					
CF	☐	☐	☐	☐		4.00		Undefined	Undefined

Code	Minimum changes	Dissallow Unicode-characters	No personal info	No sequences or patterns	Blacklist/No dictionary words
BD		☐	☐	☐	☐
BE		☐	☐	☐	☐
BF		☐	☐	☐	☐
BG	Undefined	☐	☐	☐	☐
BH		☐	☐	☐	☐
BI		☑	☑	☐	☐
BJ		☑	☑	☐	☐
BK	Undefined	☑	☐	☐	☑
BL		☐	☑	☐	☐
BM		☑	☑	☐	☐
BN		☑	☑	☐	☐
BO		☑	☑	☐	☐
BP		☐	☑	☐	☑
BQ		☐	☐	☐	☐
BR		☐	☐	☐	☐
BS		☐	☑	☐	☐
BT		☐	☐	☐	☐
BU		☐	☐	☐	☐
BV		☐	☑	☐	☐
BW		☐	☑	☐	☑
BX		☐	☐	☐	☐
BY		☑	☑	☐	☑
BZ		☐	☑	☐	☐
CA		☑	☑	☑	☑
CB		☐	☐	☐	☐
CC		☐	☑	☑	☐
CD	4	☑	☑	☑	☑
CE		☐	☐	☐	☐
CF		☐	☑	☐	☐

Code	MFA w/ password	Safe to write down	Enacted	Valid through
BD	☐			
BE	☐		2016	
BF	☐			
BG	☐	No	2023	
BH	☐		2016	
BI	☐		2023	
BJ	☐	No		
BK	☐			
BL	☐		2024	
BM	☐			
BN	☐			
BO	☐		2020	Revised as needed
BP	☐			
BQ	☐		2005	
BR	☐			
BS	☐		2020	
BT	☐		2021	
BU	☐			
BV	☐	Safe	2018	2022
BW	☐	Safe	2023	
BX	☐	No	2021	2021-09-27
BY	☐		2020	
BZ	☐	Safe	2021	
CA	☐	Safe		
CB	☐	Safe	2020	Revisions every 6 months
CC	☐	Safe		
CD	☑	No	2023	
CE	☐			
CF	☐	Safe	2010	

Code	Passwordless	No policy document	Rejected	Förbund/Delar	Min Length	Char classes	Login attempts	Password cycle	Password history
CG	☐	☐	☐	☐	8.00	4.00	5	30	Undefined
CH	☐	☐	☐	☐	10.00	4.00			
CI	☐	☐	☐	☐	8/10/12	2.00		60/75/90	
CJ	☐	☐	☐	☐	8.00	3.00			
CK	☐	☐	☐	☐	11.00	3.00		365	11
CL	☐	☐	☐	☐		3.00		90	
CM	☐	☐	☐	☑	8.00	Undefined		90	24
CN	☑	☐	☐	☐					
CO	☐	☐	☐	☐	12.00	4.00	3	120	Undefined
CP	☐	☐	☐	☑	14.00	3.00			Undefined
CQ	☐	☐	☐	☐	15.00	4.00			
CR	☐	☐	☐	☐	16.00	3.00		No	12
CS	☐	☐	☐	☐	16.00		5		
CT	☐	☐	☐	☑	14.00	3.00			Undefined
CU	☐	☑	☐	☐	12.00	3.00		90	
CV	☐	☐	☐	☐	8.00			180	24
CW	☐	☐	☐	☑	12.00	3.00		180	5
CX	☐	☐	☐	☐	10.00	3.00		180	Undefined
CY	☐	☐	☐	☐	8.00	3.00	3		Undefined
CZ	☐	☐	☐	☐	8.00	3.00		180	
DA	☐	☐	☐	☐	12.00	3.00	5	Undefined	
DB	☐	☑	☐	☐	12.00	3.00	5	360	Undefined
DC	☐	☐	☐	☐	8.00	3.00		90	
DD	☐	☐	☐	☐	8.00	3.00	5	360	Undefined
DE	☐	☐	☐	☐	12.00			180	
DF	☐	☐	☐	☑	14.00	3.00			Undefined
DG	☐	☐	☐	☑	14.00	3.00			Undefined
DH	☐	☐	☐	☐	11.00	3.00	Undefined	180	Undefined
DI	☐	☐	☐	☐	8.00	3.00	Undefined	90	Undefined

Code	Minimum changes	Dissallow Unicode-characters	No personal info	No sequences or patterns	Blacklist/No dictionary words
CG		☐	☐	☐	☐
CH		☐	☐	☐	☐
CI		☐	☐	☐	☐
CJ	Undefined	☑	☑	☐	☐
CK		☑	☑	☐	☐
CL		☐	☐	☐	☐
CM		☐	☐	☐	☐
CN		☐	☐	☐	☐
CO		☐	☐	☐	☐
CP		☐	☑	☐	☑
CQ		☐	☑	☑	☑
CR		☐	☑	☐	☐
CS		☐	☑	☐	☐
CT		☐	☑	☐	☑
CU		☐	☐	☐	☐
CV		☐	☑	☐	☐
CW	3	☐	☑	☐	☐
CX		☐	☑	☑	☑
CY		☑	☑	☐	☐
CZ		☑	☑	☐	☐
DA		☑	☑	☐	☐
DB		☐	☑	☐	☐
DC		☐	☐	☐	☐
DD		☐	☑	☐	☐
DE	2	☑	☑	☑	☐
DF		☐	☑	☐	☑
DG		☐	☑	☐	☐
DH		☐	☑	☐	☐
DI		☐	☐	☐	☐

Code	MFA w/ password	Safe to write down	Enacted	Valid through
CG	☐		2021	
CH	☐			
CI	☐	No		
CJ	☐			
CK	☐	Safe	2022	
CL	☐			
CM	☐			
CN	☐			
CO	☐		2012	Until further notice
CP	☐		2022	
CQ	☐			
CR	☐		2022	
CS	☐		2022	Until further notice
CT	☐		2022	
CU	☐	No	2022	
CV	☐	Safe	2019	
CW	☐	No	2023	Until further notice
CX	☐		2022	
CY	☐	No	2019	Until further notice
CZ	☐	Safe	2018	
DA	☐	No	2022	
DB	☐			
DC	☐		2013	
DD	☐	Safe	2019	
DE	☐	No	2021	
DF	☐		2022	
DG	☐		2022	
DH	☐		2021	
DI	☐		2015	

Code	Passwordless	No policy document	Rejected	Förbund/Delar	Min Length	Char classes	Login attempts	Password cycle	Password history
DJ	☐	☐	☐	☐	12.00	3.00			
DK	☐	☐	☐	☑	8.00	Undefined		90	24
DL	☐	☐	☐	☐	12.00	2.00		365	10
DM	☐	☐	☐	☐	12.00			Undefined	Undefined
DN	☐	☐	☐	☑	8.00	Undefined		90	24
DO	☐	☐	☐	☐	6.00	2.00		Undefined	Undefined
DP	☐	☐	☐	☐	12.00	3.00		180	5
DQ	☐	☐	☐	☐	16.00		12	No	12
DR	☐	☐	☐	☑	8.00	3.00	3	90	Undefined
DS	☐	☐	☐	☑	12.00	3.00	5	365	
DT	☐	☐	☐	☐	10.00	3.00			Undefined
DU	☐	☐	☐	☑	12.00	3.00			
DV	☐	☐	☐	☐	8.00		3	100	Undefined
DW	☐	☐	☐	☐	12.00	4.00		90	
DX	☐	☐	☐	☐		4.00	5	Undefined	
DY	☐	☐	☐	☐	10.00	3.00	Undefined	730	Undefined
DZ	☐	☐	☐	☐	8.00	3.00		120	
EA	☐	☐	☐	☐	10.00	4.00		Undefined	
EB	☐	☐	☐	☑	12.00	3.00			
EC	☐	☐	☐	☐	12.00	4.00		730	5
ED	☐	☑	☐	☐	10.00	3.00		180	24
EE	☐	☐	☐	☐	14.00	3.00		730	24
EF	☐	☐	☐	☑	12.00	3.00	5	365	
EG	☐	☐	☐	☐	8.00	3.00		90	13
EH	☐	☐	☐	☐	8.00	3.00			
	2								

Code	Minimum changes	Dissallow Unicode-characters	No personal info	No sequences or patterns	Blacklist/No dictionary words
DJ		☐	☑	☐	☑
DK		☐	☐	☐	☐
DL		☑	☐	☐	☐
DM		☑	☑	☐	☐
DN		☐	☐	☐	☐
DO		☑	☑	☐	☐
DP	3	☐	☑	☐	☐
DQ	4	☑	☑	☑	☑
DR		☐	☐	☐	☐
DS		☑	☑	☑	☑
DT		☑	☑	☐	☐
DU		☐	☑	☑	☐
DV		☐	☑	☑	☑
DW		☐	☑	☐	☑
DX		☐	☑	☐	☐
DY		☐	☑	☑	☑
DZ		☐	☑	☐	☐
EA		☐	☐	☐	☐
EB		☐	☑	☑	☐
EC		☑	☑	☑	☐
ED	1*	☑	☑	☐	☑
EE		☐	☐	☐	☐
EF		☑	☑	☑	☑
EG		☑	☑	☑	☐
EH		☐	☑	☑	☑

Code	MFA w/ password	Safe to write down	Enacted	Valid through
DJ	☑		2023	
DK	☐			
DL	☐			
DM	☐		2018	
DN	☐			
DO	☐	No		
DP	☐	No	2023	Until further notice
DQ	☑	No	2023	
DR	☐		2016	
DS	☐		2022	
DT	☐	Safe	2024	
DU	☐	Safe		
DV	☐	Safe	2010	
DW	☐	No	2021	
DX	☐	Safe	2016	
DY	☐		2019	Until further notice
DZ	☐		2021	2026-12-31
EA	☐	Safe	2022	
EB	☐	Safe		
EC	☐	No	2020	
ED	☐			
EE	☐			
EF	☐		2022	
EG	☐	Safe	2021	Until further notice
EH	☐	Safe	2024	

B.4 Dataset 2 old

Code	Min Length	Char classes	Login attempts	Password cycle	Password history	Minimum changes	Dissallow Unicode-characters
AF	6.00	4.00		90.00	Undefined		☐
AO		4.00		Undefined	Undefined		☐
AP	8.00	2.00	3.00	Undefined			☑
AQ	6.00	3.00		90.00			☐
AR	8.00	Undefined		365.00	24		☐
AS	8.00			90.00			☑
AT							☐
AU	8.00	3.00		Undefined	Undefined		☐
BI	10.00			90.00			☐
BK	8.00	3.00			Undefined	Undefined	☑
BN	8.00	3.00		90.00			☐
BO							☐
BT	12.00	2.00		90.00	30 / 1 year		☐
BV	6.00			Undefined			☐
BW	8.00	4.00		90.00	1 year		☐
BX				90.00			☑
BY	6.00	4.00	5.00	90.00	Undefined		☐
CB	14.00	4.00					☐
CE	10.00	3.00			Undefined		☑
CG	8.00	4.00	3.00	30.00	Undefined		☐
CN	10.00	3.00			Undefined		☑
CR	8.00						☐
CU	8.00	3.00		90.00			☐
CX	10.00	3.00		180.00	Undefined		☐
DA	12.00	3.00	5.00	Undefined	Undefined		☑
DB	8.00	3.00	5.00	360.00	Undefined		☐
DD	8.00	3.00	5.00	360.00	Undefined		☐
DF	8.00	2.00					☐
DH	8.00	3.00		90.00	Undefined		☐

Code	No personal info	No sequences or patterns	Blacklist/No dictionary words	MFA w/ password	Safe to write down	Enacted
AF	☑	☐	☐	☐		2009
AO	☑	☐	☐	☐	Safe	2008
AP	☑	☐	☐	☐		2008
AQ	☐	☐	☐	☐		2002
AR	☐	☑	☐	☐		
AS	☑	☑	☐	☐		2006
AT	☐	☐	☐	☐		
AU	☑	☐	☐	☐	Safe	2019
BI	☐	☐	☐	☐		
BK	☐	☐	☑	☐		2022
BN	☑	☐	☐	☐	Safe	2019
BO	☑	☐	☐	☐	Safe	2004
BT	☐	☐	☐	☐		2019
BV	☑	☑	☐	☐	Safe	2005
BW	☐	☐	☐	☐		2021
BX	☐	☐	☐	☐		2004
BY	☑	☐	☐	☐		2013
CB	☐	☐	☐	☐		2020
CE	☐	☐	☐	☐		
CG	☐	☐	☐	☐		2009
CN	☐	☐	☐	☐		
CR	☐	☐	☐	☐		2019
CU	☐	☐	☐	☐	No	2019
CX	☐	☑	☑	☐		2021
DA	☐	☐	☐	☐	No	2019
DB	☑	☐	☐	☐		2016
DD	☑	☐	☐	☐		2018
DF	☐	☐	☐	☐		
DH	☐	☐	☐	☐		

Code	Valid through		
AF			
AO			
AP			
AQ			
AR			
AS			
AT			
AU			
BI			
BK			
BN			
BO			
BT			
BV			
BW			
BX			
BY			
CB	Revision every 6 months		
CE	Revised as needed		
CG			
CN			
CR			
CU			
CX			
DA			
DB			
DD			
DF			
DH			

Code	Min Length	Char classes	Login attempts	Password cycle	Password history	Minimum changes	Dissallow Unicode-characters
DJ	12.00	2.00			Undefined		☐
DL	16.00			90.00			☐
DP	8.00	4.00		90.00	5		☐
DT	10.00	3.00			Undefined		☑
DW	8.00	4.00		90.00			☐
EA	6.00		3.00	40.00			☐
EH	8.00	3.00					☐

Code	No personal info	No sequences or patterns	Blacklist/No dictionary words	MFA w/ password	Safe to write down	Enacted
DJ	☑	☐	☐	☐	Safe	2021
DL	☐	☐	☐	☐		
DP	☑	☑	☐	☐	No	2021
DT	☑	☐	☐	☐	Safe	2022
DW	☑	☐	☑	☐	No	
EA	☑	☑	☑	☐		2007
EH	☑	☑	☑	☐	Safe	2022

Code	Valid through	
DJ		
DL		
DP	Until further notice (review 2022-09-01)	
DT		
DW		
EA		
EH		

C 8388-2024-1

Länsstyrelsen
Västra Götaland

Enheten för samhällsskydd
och beredskap

Information och lägesbild 2024-02-28

Dnr. 457- 8388-2024

Sida 1(1)

Ökat antal inhämtningsförsök av känslig information

Den senaste tiden har kommuner i länet haft dialog med Länsstyrelsen Västra Götaland, om ett ökat antal aktiviteter som skulle kunna misstänkas utgöra inhämtningsförsök av känslig information. Det har handlat om exempelvis:

- begäran om olika typer av fakturor, bland annat för reservkraft
- enkät/frågor om reservkraftsförmåga
- enkätfrågor från studenter om våldsbejakande extremism, kommunens lösenordspolicy eller frågor om dricksvatten – frågorna kommer både från högskolemejl och från andra mejladresser
- mejl med hot om att publicera uppgifter i media, där avsändaren felaktigt uppger sig vara journalist.

Var uppmärksam och iaktta försiktighet

Vi vill med denna information mana kommuner i länet att vara extra uppmärksamma på den här typen av aktiviteter och att vara försiktiga med hur de hanteras. Samhällsläget och bland annat Sveriges pågående Natoprocess har gjort att antalet påverkansförsök och cyberangrepp mot Sverige och svenska samhällsaktörer har ökat. Det är tänkbart att också inhämtningsförsök från främmande makt ökar i samband med detta.

Det är viktigt att vi som myndigheter säkerställer den grundlagsskyddade rättigheten för allmänhet och media att ta del av allmänna handlingar – men att vi samtidigt skyddar det skyddsvärda.

Rapportera till Länsstyrelsen

Misstänker ni att ni utsatts/utsätts för inhämtningsförsök, rapportera detta till Länsstyrelsen senast fredag den 1 mars. Det hjälper till att skapa en helhetsbild av läget i länet. Vi delar den övergripande lägesbilden i vår regelbundna rapportering till MSB.

- Meddela om ni fått vad ni uppfattar som inhämtningsförsök (under 2024).
- Om ja, vilken typ av inhämtningsförsök?
- Var noga med att skriva på ett sätt som inte röjer sekretess.
- Vid frågor kontakta Länsstyrelsen, lisa.nordahl@lansstyrelsen.se

Rapportera till: samhallsstorning.vastragotaland@lansstyrelsen.se

Postadress: 403 40 Göteborg Telefon: 010-224 40 00 (vxl) Webb: www.lansstyrelsen.se/vastragotaland E-post: vastragotaland@lansstyrelsen.se

D Inter-rater reliability

Length

	8	10	6		12	5	16	14	11	9	15	8/10/12	17	14/8	20/	8/8/12	Sum
8	76.00			2.00			1.00										79.00
10	2.00	9.00		1.00													12.00
6			6.00														6.00
		1.00		9.00													10.00
12					37.00												37.00
5			1.00														1.00
16							6.00										6.00
14								12.00									12.00
11									3.00								3.00
9										1.00							1.00
15											4.00						4.00
8/10/12																1.00	1.00
17													1.00				1.00
14/8				1.00													1.00
20/				1.00													1.00
8/8/12																	0.00
Sum	78.00	10.00	7.00	14.00	37.00	0.00	7.00	12.00	3.00	1.00	4.00	0.00	1.00	0.00	0.00	1.00	

Total	Agreements	Po	Pe	k
175	164	0.9371428571	0.2627265306	0.9147437885

Klasser

	1	2	3	4		Undefined	No	1/3	Undefined / 1	Sum
1		1.00								1.00
2		9.00	4.00		2.00					15.00
3			74.00	5.00	3.00	1.00				83.00
4			16.00	27.00						43.00
	2.00		3.00		17.00				1.00	23.00
Undefined					6.00					6.00
No							2.00			2.00
1/3					2.00					2.00
Undefined / 1										0.00
Sum	2.00	10.00	97.00	32.00	30.00	1.00	2.00	0.00	1.00	

Total	Agreements	Po	Pe	k
175	129	0.7371428571	0.3356408163	0.6043448344

Inloggningsförsök

	3	5	6	10	12		Undefined	Sum
3	9.00					7.00		16.00
5		16.00				4.00		20.00
6			1.00					1.00
10				7.00				7.00
12					2.00			2.00
	2.00	3.00				119.00	2.00	126.00
Undefined						1.00	2.00	3.00
Sum	11.00	19.00	1.00	7.00	2.00	131.00	4.00	

Total	Agreements	Po	Pe	k
175	156	0.8914285714	0.5592816327	0.753648959

Dagar mellan byt

	30	360		90	180	40	365	120	Undefined	730	No	45/90	60/75/90	100	180-270	60	No/Undefined	46	Sum
30	2.00																		2.00
360		4.00																	4.00
		1.00	42.00	3.00	1.00				5.00										52.00
90			1.00	43.00				1.00	1.00										46.00
180			1.00		13.00														14.00
40						1.00													1.00
365							11.00		2.00										13.00
120				1.00			3.00												4.00
Undefined			3.00						12.00										15.00
730										4.00									4.00
No											2.00								2.00
45/90																		1.00	1.00
60/75/90													1.00						1.00
100														1.00					1.00
180-270					6.00														6.00
60																7.00			7.00
No/Undefined			2.00																2.00
46																			0.00
Sum	2.00	5.00	49.00	47.00	20.00	1.00	14.00	1.00	20.00	4.00	2.00	0.00	1.00	1.00	0.00	7.00	0.00	1.00	

Total	Agreements	Po	Pe	k
175	143	0.8171428571	0.1819428571	0.7764738754

Lösenordshistorik

	Undefined		1år	24	5	30/1år	12	10	13	6	24/1år	11	8	30	Sum
Undefined	38.00	7.00													45.00
	11.00	79.00		1.00			1.00								92.00
1år			1.00												1.00
24		2.00		17.00											19.00
5					4.00										4.00
30/1år														2.00	2.00
12		1.00					2.00								3.00
10								3.00							3.00
13									1.00						1.00
6		1.00								1.00					2.00
24/1år				1.00											1.00
11												1.00			1.00
8													1.00		1.00
30															0.00
	49.00	90.00	1.00	19.00	4.00	0.00	3.00	3.00	1.00	1.00	0.00	1.00	1.00	2.00	

Total	Agreements	Po	Pe	k
175	148	0.8457142857	0.3554612245	0.7606261715

Minimum changes

	3	4	2*	2	Undefined	1		Sum
3	2.00							2.00
4		2.00						2.00
2*			2.00					2.00
2			1.00			5.00		6.00
Undefined								0.00
1								0.00

			1.00		5.00		157.00	163.00
	2.00	2.00	4.00	0.00	5.00	5.00	157.00	

Total	Agreements	Po	Pe	k
175	163	0.9314285714	0.8361469388	0.5815065763

Disallow unicode

	TRUE	FALSE	Sum
TRUE	43.00	11.00	54.00
FALSE	2.00	119.00	121.00
Sum	45.00	130.00	

Total	Agreements	Po	Pe	k
175	162	0.9257142857	0.5929795918	0.8174889691

No sequences

	TRUE	FALSE	Sum
TRUE	27.00	8.00	35.00
FALSE	6.00	134.00	140.00
Sum	33.00	142.00	

Total	Agreements	Po	Pe	k
175	161	0.92	0.6868571429	0.7445255474

MFA \w pass

	TRUE	FALSE	Sum
TRUE	1.00	13.00	14.00
FALSE	2.00	159.00	161.00
Sum	3.00	172.00	

Total	Agreements	Po	Pe	k
175	160	0.9142857143	0.9056	0.09200968523

Write down

	No	Safe		Sum
No	21.00		10.00	31.00
Safe	21.00	2.00	7.00	30.00
	13.00	1.00	100.00	114.00
Sum	55.00	3.00	117.00	

Total	Agreements	Po	Pe	k
175	123	0.7028571429	0.4941387755	0.4126000516

No personal info

	TRUE	FALSE	Sum
TRUE	84.00	10.00	94
FALSE	15.00	66.00	81
Sum	99	76	

Total	Agreements	Po	Pe	k
175	150	0.8571428571	0.5048816327	0.7114687067

Blacklist

	TRUE	FALSE	Sum
TRUE	32.00	11.00	43
FALSE	4.00	128.00	132
Sum	36	139	

Total	Agreements	Po	Pe	k
175	160	0.9142857143	0.6496653061	0.7553360052

Pooled kappa

PoAve	PeAve	kPool
0.8661904762	0.5304435374	0.7150299602

E Translations

E.1 Law

rikets säkerhet eller dess förhållande till en annan stat eller en mellanfolklig organisation,
“The security of the kingdom or its relation to another state or organization.”

rikets centrala finanspolitik, penningpolitik eller valutapolitik,
“The central financial politics, monetary politics, or exchange rate policies of the kingdom.”

myndigheters verksamhet för inspektion, kontroll eller annan tillsyn,
“Government agencies for inspection, control, or other supervisions.”

intresset av att förebygga eller beivra brott,
“The interest of preventing and prosecuting crime.”

det allmännas ekonomiska intresse,
“The common economic interest.”

skyddet för enskildas personliga eller ekonomiska förhållanden…
“The protection of individuals’ personal or economical condition.”

intresset av att bevara djur- eller växtart.
“The interest to preserve animal or plant species.”

E.2 Deductive coding

”Lösenordet ska bestå av minst 8 tecken”
“The password shall consist of at least 8 characters”

”Ditt lösenord ska bestå av minst 14 tecken där både gemener (små bokstäver) och versaler (stora bokstäver) används.”
“Your password shall consist of at least 14 characters in which both minuscule (lower case letters) and majuscule (upper case letters) characters are used. ”

”Lösenordet ska innehålla tecken från 3 av följande 4 kategorier.”
“The password shall contain characters from 3 out of 4 categories.”

”Efter tre misslyckade försök att logga in spärras kontot.”
“After three failed login attempts, the account is locked.”

”Byte av lösenord är aktuellt var 30:e dag när det gäller interna nätverket. En dialogruta visas på skärmen när det är dags.”
“Password changes are scheduled every 30 days for the internal network. A dialog popup will show up on the screen when it is time.”

”IT-systemen i produktion ska kunna tvinga fram byte av lösenord på begäran (omedelbart) eller inom ställda tidsramar.”
“The IT-systems in production shall be able to force a password change on demand (immediately) or within a set time frame.”

”Inte samma som de senaste 24 lösenorden.”
“Not the same as the last 24 passwords.”

”Inte återanvända samma lösenord inom 1 år.”
“Not reuse the same password within 1 year.”

”måste skilja sig från det senaste lösenordet med mer än det sista tecknet.”
“Must differ from the last password with more than the last character”

”Vid byte av lösenord måste minst fyra tecken bytas.”
“At least four characters must be changed during a password change.”

“Datum 2019-10-16.”
“Date 2019-10-16”

“Fastställd/upprättad 2023-09-20 av IT-chef”
“Established 2023-09-20 by the head of IT”

”Giltighetstid: Tills vidare + Första översyn 2022-09-01”
“Period of validity: Until further notice + First review 2022-09-01”

”Giltig till 2026-12-31.”
“Valid until 2026-12-31”

E.3 Inductive coding

”Stora bokstäver [A-Z]”
“Capital letters [A-Z]”

“Undvik å, ä eller ö i lösenord”.
“Avoid the use of å, ä, or ö in passwords”

”Lösenordet får inte innehålla användarens förnamn, efternamn, kontonamn, e-postadress eller andra uppgifter som lätt kan kopplas till användaren”
“Passwords shall not contain the user’s first name, last name, username, e-mail, or other pieces of information that can easily be connected to the user.”

”Undvik lösenord som kan associeras med din person”.
“Avoid passwords that can be associated with your person”

”Enkla repetitiva mönster som till exempel ABCD1234, AAAAAAA2 ska undvikas”
“Simple, repetitive patterns, for example ABCD1234, AAAAAAA2 shall be avoided”

”Använd inte ordet fotboll, losenord, password, hej, hejsan som del av lösenordet”
“Do not use the words fotboll, losenord, password, hej, hejsan as a part of the password”

”Använd inte årstidens namn eller dess nummer”
“Do not use the name of the season or its number”

”MFA-multifaktorsautentisering aktiverad för samtlig personal”
“MFA-multifactor authentication is activated for all personnel”

”Windows Hello är aktiverat som standard”
“Windows Hello is activated as standard”

”Användare som arbetar på distans identifierar sig med användarnamn samt autentiserar sig med lösenord och med erhållen kod till egen, personlig enhet (2-faktors autentisering)”
“Users who work remotely identify themselves with a username, and authenticate themselves with a password and with a code for their own personal device (2-factor authentication)”

”Ytterligare metoder för inloggning kan vara att använda sig av bank-id eller mobilt bank-id eller säkra kort, exempelvis SITHS-kort”
“Additional methods for signing in can be the use of bank-id or mobile bank-id, or safe cards, for example SITHS-card”

”Utifrån systemens säkerhetsklassning kan andra krav ställas på inloggning. För vissa system krävs inloggning med tvåfaktorsautentisering som innebär att man förutom ett lösenord till exempel kan behöva ta emot sms med en kod för inloggning”.
“Depending on the security classifications of the system, other requirements can be applied for login. For some systems, two-factor authentication is required which implies that in addition to a password, an sms needs to be received with a code for logging in, for example.“

”Lösenord ska hanteras som en värdehandling”
“Passwords shall be handled as an important document”

”Skriv inte ner lösenordet om du inte kan förvara det säkert”
“Do not write the password down if you cannot store it safely”

”Skriv inte upp ditt lösenord någonstans”
“Do not write your password down anywhere”