Report author: Abi Dakin
Tel: 07793 742898

Report of Director of Resources and Housing
Report to Corporate Governance and Audit Committee

Date: 28th January 2018

Subject: Information Management and Governance – Update on the Password Protocol for Network ID.

Are specific electoral wards affected? If yes, name(s) of ward(s):	☐ Yes ☒
Are there implications for equality and diversity and cohesion and integration?	☐ Yes ☒ No
Is the decision eligible for call-in?	☐ Yes ☒ No
Does the report contain confidential or exempt information? If relevant, access to information procedure rule number:	☐ Yes ☒ No

Summary of main issues

1. Following the publication of the National Cyber Security Centre's password guidance, 'Simplifying your approach', the password policy for Leeds City Council Network ID was reviewed. It was decided to update the password policy to a protocol under a renewed policy document set and the improvements were approved by CLT on the 23rd May 2017.

2. In the same year KPMG's audit on key systems security, which forms an element of the wider finance audit, found that for two key financial systems and their associated infrastructure, the technical password policies were not fully aligned to the original LCC Password Policy.

3. This report provides an update on the Council's response to the issues and more generally reports on work to increase the robustness of the Council's Password Policy.

Recommendations

Corporate Governance and Audit Committee is asked to consider the contents of this report and be assured of the Council's approach to the controls around access to the LCC Network ID, the password protocol and the progress so far in implementing the protocol.

1. Purpose of this report

1.1 To provide Corporate Governance and Audit Committee with an update on the arrangements in place regarding the LCC Network ID Password Protocol, whether up to date, fit for purpose, effectively communicated, routinely complied with and monitored.

2. Background information

2.1 Authentication to systems, services and data is one of the ways in which we ensure that only appropriate users access our information assets. The main method of authentication for LCC users is the Network ID. The user name and password.

2.1 From April 2018, the LCC password protocol improvements are now in-line with National Cyber Security Centre (NCSC) guidance. This prevents the use of extremely weak passwords found on global lists.

2.2 In 2016, the NCSC published new guidance around passwords, the psychology of a user and the technical controls that should be implemented around controlling access to systems. These documents detailed efforts that should be made to reduce the challenge to the person logging in and as a result discourage the urge to write passwords down, which is evidenced to improve overall security. (see Appendix 1) LCC password Protocol is based on those recommendations.

2.3 As part of the Council's IT Health Check (ITHC), an annual audit of the Council's security arrangements a password audit was completed. This still discovered a number of weak passwords.

2.4 Grant Thornton have been appointed as the Council's External Auditor from 2018/19 to deliver the Financial audit, incorporating an audit on Key financial systems and basic, entity controls across the technical infrastructure. This includes adherence to Council Protocol and a review of Best Practice

3. Main issues

3.1 The Head of Information Management and Governance took a paper to Corporate Leadership Team on 23rd May 2017 to agree the fundamental change in passwords for LCC. This change brings the protocol in line with NCSC guidance.

3.2 The new protocol follows the guidance issued by the NCSC, reducing the probability of a person using a single dictionary word and single number as their password as the method to authenticate the 'User to the device', but also to discourage the human element of writing down a password that is not memorable, one that is too complex, or due to having to remember a number of different passwords. It is also hoped due to the format of the password, users will be discouraged from using their work password for systems outside of the work environment.

3.3 To reduce the number of passwords a user is required to remember, the protocol mandates Single Sign-On to access subsidiary systems where possible. This technology turns the password into a token, which is then exchanged with the secondary system in place of a second password. It also mitigates the risk of a user accessing the secondary system with another person's details, bypassing the segregation of duties controls held within the system itself, reducing the risk of internal fraud.

3.4 Following the usual commissioning and change processes, alterations made to the Password Protocol were communicated to coincide with the updated, mandatory Information Governance training in April 2018.

3.5 Standard User accounts have been addressed in stages, from April, concluding in a forced password reset for the remaining support and elected member accounts throughout September.

3.6 ADM accounts or admin' accounts, those with raised privileges, began the same process in mid-September.

3.7 Another, invisible, control has been commissioned by Digital Information Services using the certificate on Council devices. This introduces a second method of authentication of the 'device to the network', preventing the use of unmanaged devices on the network, reducing the risk that unpatched devices can bring. This Network Access Control (NAC) solution is in the latter stages of implementation. Thus providing the additional security of Two Factor (2FA) to the Leeds Network.

3.8 Prior to the appointment of Grant Thornton, KPMG was the appointed External Auditor for the Council. Their audit of financial statements found that, for two key financial systems, and their associated infrastructure, the technical password policies were not fully aligned with Corporate Protocol. They are SAP (HR system) and FMS (Financial Management). Changes to these technical password policies have been made to bring them to compliance with the protocol. Portfolio requests have been raised to address the issue of Single Sign On in both cases.

3.9 Since Grant Thornton's appointment dialogue has continued on this issue and in light of discussions a further revision to the Password protocol has been made. This has established a minimal password length for access to secondary systems that cannot meet the Single Sign-on requirement.

3.10 Information Governance and Information Security will continue to monitor password usage via the ITHC audit, annually. A password blacklisting tool will be commissioned as part of 2018/19 work to further prevent the use of common/known passwords. The blacklist contains a database of commonly used passwords and phrases which will prevent the user from making a poor password choice.

4. Corporate considerations

4.1 Consultation and engagement

4.1.1 Consultation on the development of strategies, protocols, policies, procedures and standards are extensively undertaken across a broad range of stakeholders including information management professionals, representatives from all directorates via representatives of Information Management and Technology Teams and Information Management Board members. In the case of the Password Protocol, additional consultation was held with the National Cyber Security Centre, the Cabinet Office, Security partners, Surecloud and auditors KMPG and now Grant Thornton

4.2 Equality and diversity / cohesion and integration

4.2.1 Equalities, diversity, cohesion and integration are all being considered as part of delivering the Information Management and Governance Strategy. This refers to the way training is being delivered as well as how policies will impact on staff and partners.

4.3 Council policies and best council plan

4.3.1 All information governance related policies are currently being reviewed and a dedicated Policy Review group has been established. As part of this review the group will be consulting with internal stakeholders and external peer checking.

4.4 Resources and value for money

4.4.1 There are no specific implications arising from this report.

4.5 Legal implications, access to information, and call-in

4.5.1 Delegated authority sits with the Director of Resources and Housing and Senior Information Risk Owner and has been sub-delegated to the Chief Information Officer under the heading “Knowledge and information management” in the Director of Resources and Housing Sub-Delegation Scheme.

4.5.2 Restrictions as to the nature of the Council’s authentication methods should be considered seriously as they may be used to scope a Cyber Attack on Council systems.

4.6 Risk management

4.6.1 The benefits of full implementation of the password protocol will reduce user burden, which increases security. It will also reduce the sharing of passwords between work accounts and home accounts, increase the security of the network and the systems protected by it and reduce the risk of cyber-attack. Should the password protocol not be implemented in full, across all users and secondary systems the benefits proposed will not be realised in full.

4.6.2 A long and strong approach to passwords reduces the overall risk of unauthorised access to Leeds City Council Networks by brute force attack and from those writing down their password, or using the same password across numerous systems due to its’ length.

5. Conclusions

5.1 The establishment of strengthened authentication methods including alterations to the Password protocol have improved the Council’s security posture and continue to protect the environment, alongside additional measures to incorporate controls against unmanaged device access. This means Leeds City Council devices and authorised users can access the network and the data it protects.

5.2 Secondary systems unable to meet the requirements of the protocol have work requests logged and will follow the amended password protocol until Single Sign-On can be implemented.

6. Recommendations

6.1 Corporate Governance and Audit Committee is asked to consider the contents of this report and be assured of the Council's approach to the controls around access to the LCC Network, and the password protocol.

7. Background documents[1]

None.

[1] The background documents listed in this section are available to download from the Council's website, unless they contain confidential or exempt information. The list of background documents does not include published works.

Appendix 1

Extracts from the National Cyber Security Centre's guidance on simplifying your approach to passwords. https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

Attackers use a variety of techniques to discover passwords. Many of these techniques are freely available and documented on the Internet, and use powerful, automated tools. LCC have assessed the threat from each of the types of attack and written the Password Protocol to address each.

Threat	LCC Mitigation
Social engineering eg phishing; coercion	Protocol, training and communication, 2 Factor Authentication.
Manual password guessing, perhaps using personal information 'cribs' such as name, date of birth, or pet names	Protocol, guidance on selecting random words, training, 2 Factor Authentication.
Intercepting a password as it is transmitted over a network	Passwords are encrypted in the Active Directory, which requires the highest privilege and a BPSS check. Authentication processes are also encrypted. Caching (storing) of passwords on council systems is disabled. 2 Factor Authentication.
'Shoulder surfing', observing someone typing in their password at their desk	Length of password
Installing a keylogger to intercept passwords when they are entered into a device	Endpoint protection installed on user devices, background scanning. 2 factor authentication
Searching an enterprise's IT infrastructure for electronically stored password information	Ferret tool has been used for audit of password data 2 factor authentication
Brute-force attacks; the automated guessing of large numbers of passwords until the correct one is found	Number of attempts to guess password locks out at ten attempts 2 factor authentication
Finding passwords which have been stored insecurely, such as handwritten on paper and hidden close to a device	Removal of requirement to change passwords, unless compromised. Single password for Network ID and secondary systems. Single Sign On. 2 Factor Authentication
Compromising databases containing large numbers of user passwords, then using this information to attack other systems where users have	Passwords are not stored in plain text, in that they are hashed, a type of encryption that cannot be reversed, where possible a 'salt' is applied before the hash, which

re-used these passwords.	prevents further attacks. 2 Factor authentication

NCSC extract

Changing passwords

Most administrators will force users to change their password at regular intervals, typically every 30, 60 or 90 days. This imposes burdens on the user (who is likely to choose new passwords that are only minor

Searching an enterprise's IT infrastructure for electronically stored password information	Ferret tool has been used for audit of password data 2 factor authentication
Brute-force attacks; the automated guessing of large numbers of passwords until the correct one is found	Number of attempts to guess password locks out at ten attempts 2 factor authentication
Finding passwords which have been stored insecurely, such as handwritten on paper and hidden close to a device	Removal of requirement to change passwords, unless compromised. Single password for Network ID and secondary systems. Single Sign On. 2 Factor Authentication
Compromising databases containing large numbers of user passwords, then using this information to attack other systems where users have re-used these passwords.	Passwords are not stored in plain text, in that they are hashed, a type of encryption that cannot be reversed, where possible a 'salt' is applied before the hash, which prevents further attacks. 2 Factor authentication

NCSC extract

Changing passwords

Most administrators will force users to change their password at regular intervals, typically every 30, 60 or 90 days. This imposes burdens on the user (who is likely to choose new passwords that are only minor variations of the old) and carries no real benefits as stolen passwords are generally exploited immediately. Long-term illicit use of compromised passwords is better combated by:

- monitoring logins to detect unusual use
- notifying users with details of attempted logins, successful or unsuccessful; they should report any for which they were not responsible

Regular password changing harms rather than improves security, so avoid placing this burden on users. However, users must change their passwords on indication or suspicion of compromise.