APPENDIX 8

Access and Security Protocol

May 2018

1. Policy Statement

1.1 Tameside Metropolitan Borough Council (The Council) will establish specific requirements for protecting information and information systems against unauthorised access.

1.2 The Council will effectively communicate the need for information and information system access control.

2. Introduction

2.1 Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of the Council which must be managed with care.

2.2 Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

2.3 Formal procedures must control how access to information is granted and how such access is changed.

2.4 This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

3. Scope

3.1 This Access and Security Protocol outlines the framework for the management of Access Control within the Council.

3.2 The Access and Security Protocol applies to all employees (including system support staff with access to privileged administrative passwords), Members of the Council, temporary staff, contractual third parties, partners or agents of the Council who have access to any Information Systems or information for Council purposes.

3.3 Access control rules and procedures are required to regulate who can access the Council's information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Council information in any format, and on any device.

4. User Access Management

4.1 *Access Control*

4.1.1 Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed by the Council.

4.1.2 Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

4.1.3 User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

4.2 *User Registration*

4.2.1 A request for access to the Council's computer systems must first be submitted to the ICT Service Desk for approval. Applications for access must only be submitted if approval has been granted from the line manager

4.2.2 When an employee leaves the Council, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the ICT Service Desk

4.3 *User Responsibilities*

4.3.1 It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems by:

- Following the Password Policy Statements outlined in Section 10.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing the IT Service Desk of any changes to their role and access requirements.

5. Network Access Control

5.1 The use of modems on non-Council owned computers connected to the Council's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from ICT before connecting any equipment to the Council's network.

6. User Authentication for External Connections

6.1 Where remote access to the Council network is required, an application must be made via the ICT Service Desk. Remote access to the network must be secured by two factor authentication consisting of a username and one other component, for example encrypted devices and password protection. For further information please refer to the Mobile and Remote Working Protocol.

7. Supplier's Remote Access to the Council Network

7.1 Partner agencies or Third party suppliers must not be given details of how to access the Council's network without permission from ICT within a business case. Any changes to supplier's connections must be immediately sent to the ICT Service Desk so that access can be updated or ceased. All permissions and access methods must be controlled by ICT with assurances from the SIRO.

7.2 Partners or Third party suppliers must contact the ICT before connecting to the Council network and a log of activity must be maintained. Remote access software must be disabled when not in use.

8. Operating System Access Control

8.1 Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (4) and the Password section (10) must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.
- Displaying a general warning notice that only authorised users are allowed.

8.2 All access to operating systems is via a unique login ID that will be audited and can be traced back to each individual user. The login ID must not give any indication of the level of access that it provides to the system (e.g. administration rights).

8.3 System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

9. Application and Information Access

9.1 Access within software applications must be restricted using the security features built into the individual product. The manager of the software application is responsible for granting access to the information within the system. The access must:

- Be compliant with the User Access Management section (4) and the Password section (10).
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

10. Password Security

10.1 *Choosing Passwords*

10.1.1 Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.

10.1.2 A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

10.2 *Weak and Strong Passwords*

10.2.1 A *weak* password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

10.2.2 A *strong* password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

10.2.3 Everyone must use strong passwords with a minimum standard of:

- A minimum of seven characters.
- Contain a mix of alpha and numeric, with at least three non-alphabetic characters (i.e. numbers and/or symbols).
- More complex than a single word (such passwords are easier for hackers to crack).
- For further password guidance, click here to visit the IT Service Portal and type 'password' in the search box.

10.3 ***Protecting Passwords***

10.3.1 It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different TMBC systems.
- Do not use the same password for systems inside and outside of work.

10.4 ***Changing Passwords***

10.4.1 All user-level passwords must be changed at a maximum of every 42 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to the SUM or Information Asset Owner.

10.4.2 Users **must not** reuse the same password within 20 password changes

10.5 ***System Administration Standards***

10.5.1 The password administration process for individual Council systems is well-documented and available to designated individuals.

10.5.2 All Council ICT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users (i.e. no generic accounts).
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

11. Compliance

11.1 This Access and Security Protocol takes into consideration all applicable statutory, regulatory and contractual security requirements.

11.2 It is the responsibility of Managers to exercise appropriate controls to minimise the risk of unauthorised access and where misuse is suspected to report it via the Incident Reporting Procedure process, using the form on the Information Governance page.

11.3 It is the responsibility of all employees to ensure that they have read and comply with the conditions laid out in this protocol.

11.4 Non-compliance with this protocol could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers**.**

11.5 If any user is found to have breached this protocol, they may be subject to the Council's Disciplinary Procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

11.6 If you do not understand the implications of this protocol or how it may apply to you, please seek advice from the Risk and Insurance Team or the Council's ICT Security Officer. Manager.

12. References

12.1 This Access Control Protocol should be read in conjunction with the overall Information Governance Policy and Conduct Policy and related sub documents

12.2 The following TMBC policy documents are directly relevant to this policy, and are referenced within this document:

- Mobile and Remote Working Protocol.
- Incident Reporting Procedure.