Information Security Policy Suite

Access Control Policy

includes Remote Access and Supplier Access

ISPS - 006

This policy is available in alternative formats upon request, such as large print or electronically. Please contact the Technology Services Management Team, to obtain a copy in a different format.

v

Approval Authority: {insert approval body here}

Approval Date: xx/xx/2019

1. Purpose

The purpose of this Access Control Policy is to establish appropriate levels and methods of access to Council provided and maintained information processing systems.

2. Scope

This policy applies to all staff, Members, partners, contractors and any other persons who have authorised access to the Council's information, information systems and networks.

This policy applies to all information held, created, modified or accessed from the approval date of this policy. It includes information in any form, no matter whether it is stationary (i.e. at rest) or in transit.

3. Policy Statement

The policy of the Council is to ensure that it takes appropriate technical and organisational security measures such that:

a. Users (including suppliers) must only be provided with appropriate level access to the information systems for which they have been specifically authorised;

b. Procedures must be in place to authenticate users in accordance with the ISPS-006a Access Control Standard;

c. Procedures must be in place to ensure that any passwords used are secure.

d. Any procedures implementing security controls must be in accordance with Council requirements and those that may also be specified in service and / or data sharing agreements.

3.1 Remote Access

a. Provide secure remote access to Council services which have been approved for business purposes to eligible individuals, e.g. e-mail, internet, intranet, specific applications.

b. Will be centrally managed by the Technology Services Team.

3.1.1 Pre-Requisites

a. The individual should already have an internet connection available for remote access.

3.1.1.1 Support Arrangements

a. Telephone support will usually be available from the Service Desk (01403 215115) during normal office hours only. Anyone requiring support with Council owned, managed or assured equipment must contact the Service Desk. External technical support must not be used unless authorised by Technology Services Management.

b. Out of hours, messages can be left on the Service Desk voicemail account; these will not be checked until the next working day.

c. In the event of a problem, all Council equipment including but not limited to PCs, laptops, smart-phones, printers and routers will be supported on a return to base basis.

4. Responsibilities

As per the Information Governance and Security Policy (ISPS-001)

Additional responsibilities arising from this policy are specified below.

4.1 Senior Information Risk Owner (SIRO)

The SIRO is responsible to the Council's Chief Executive for access to the Council's network. Their responsibilities include:

a. Ensuring that access to the Council's network and relevant information systems are given to only those that need it and only as and when required.

4.2 Technology Services staff

Technology Services staff shall be responsible, via their line management, to the SIRO of Horsham District Council. They are in a privileged position due to their responsibility for administering the access to the information systems and services of the Council. Their responsibilities include:

b. Implementing and maintaining the controls detailed in this policy and standard.

c. Notifying their line manager of any deviations from the specified controls.

4.3 Technology Services Management

The Head of Technology Services is responsible to Horsham District Council's SIRO for any procurement and purchasing activities relating to remote access. Their responsibilities include:

a. Procurement of any equipment required as part of an authorised Remote Access Request.

4.4 System Administrators

Their responsibilities include:

b. User access control, managing separate logon accounts for their own systems, setting permissions and monitoring account usage.

c. Informing Technology Services when a user no longer requires access to the application(s) so that access to the system can be removed.

d. Ensuring that adequate controls are in place in conjunction with Technology Services to allow appropriate third party remote access to the Council's systems.

e. Contacting the Service Desk to notify them that a supplier has requested physical or remote access to Council systems and request assistance of the ICT Services staff if required.

f. Seeking authorisation from a member of the Technology Services management team if a supplier wishes to connect a computer or electronic device to any of the Council's Data Networks (Wired or Wireless).

g. Other administrative tasks including user system audit.

4.5 Human Resources

The Council's Human Resources responsibilities include:

a. Providing the Service Desk with a list of leavers monthly. Where the notification period is less than 1 months' notice a separate notification must be sent to ensure timely and effective network and system account suspension.

4.6 Line Managers

Line managers' responsibilities include:

a. Ensuring that notification of all starters / movers is made to the Technology Services at least three working days before access to systems is required;

b. Advising Technology Services if access to the account of someone on a temporary absence (e.g. sick, annual leave) is required and informing the individual concerned that this action was taken and the reasons for doing so.

c. Maintaining usage records in the rare instance where generic accounts are still used in their sections and working with Technology Services to remove the need for generic accounts.

d. Confirming to Technology Services that a network account may be deleted.

4.7 All Network Users

All network users responsibilities include:

a. Only accessing Council services using their own username and password;

b. Any action taken on the network under their own username;

c. Adhering to the network access authentication standards for passwords and two-factor authentication where appropriate.

d. Keeping their username, password and any security tokens issued to them secure;

e. Password used to access the Council's network must not be used for any other system (externally hosted web-based applications pose the greatest risk).

f. Not sharing any passwords provided to them for access to specific systems with other people or asking them for theirs, e.g. Revenues & Benefits system. If access is required, the individual requiring it must contact the Service Desk or

System Administrator.

g. Locking any computer, they are logged on to when it is not in use (e.g. when temporarily away from their desk);

h. Understanding that their access and/or connection to the Council's network may be monitored and logged. This is for information security investigations which may require the Council to identify accounts and / or computers that may have been compromised by external parties.

i. Immediately reporting any actual or suspected Information Security incidents such as unauthorised access in accordance with the Information Security Incident Management Policy (see section 3 of the Information Governance and Security Policy ISPS-001) and supporting procedures.

4.7.1 Remote Access

All individual users with remote access privileges responsibilities include:

a. Being aware of the Remote-working Policy (ISPS-003)) and complying with the content of each of the Information Security Polices that relate to their job role.

b. Never disclosing their passwords to anyone, particularly to family members if Council business is conducted from home.

c. Using any remote access connection to conduct Council business appropriately, responsibly, and ethically.

d. Ensuring that their computers are only connected to one network at a time.

4.8 Suppliers and Contractors

Suppliers and contractors are responsible to the Council in accordance with the initial procurement or support and maintenance contract. Their responsibilities include:

a. Complying with the Supplier Access Guidelines.

b. Only using the means of accessing systems supplied or authorised by a member of the Technology Services management team. Suppliers and contractors must not create login accounts or any other means of accessing those systems.

c. Suppliers must only access systems to which they have been granted access. Any circumvention will lead to access being removed.

d. Contact the Service desk in order to gain physical or remote access to Council systems.

e. Notifying the system administrator or Service Desk when work is complete and access no longer required.

f. Deciding through the appropriate system administrator if they wish to connect a computer or electronic device to any of the Council's Data Networks (Wired or Wireless).

g. If on site, then must allow inspection of their device to determine that it has no software or hardware posing any threat to the infrastructure or information stored on the network.

h. All contracts should go through Legal to ensure the requisite Terms and Conditions are included.

5. Training associated with this Policy

As per the Information Governance and Security Policy (ISPS-001)

6. Monitoring

As per the Information Governance and Security Policy (ISPS-001)

6.1 Non-compliance

As per the Information Governance and Security Policy (ISPS-001)

6.2 Review

As per the Information Governance and Security Policy (ISPS-001)

7. Equality Impact Assessment (EIA)

As per the Information Governance and Security Policy (ISPS-001)

8. Related documents

This policy should be read in conjunction with the following documents:

- ISPS-006b Access Control Guidelines including Supplier Access Guidelines and Declaration;
- ISPS-001 Information Governance and Security Policy;
- Other policies in the Information Security Policy Suite;
- Any supporting standards, guidelines and procedures.