U09

Remote Access Policy

Target Audience:
Manager

Contents

Document Control

Organisation	Torbay Council
Title	
Creator	Andy Booth, Network Analyst
Source	U09 Remote Access Policy (Torbay Council)
Approvals	
Distribution	
Filename	Remote Access Policy v2
Owner	Torbay IT Services / Torbay Information Governance Team
Subject	Remote Access
Protective Marking	
Review date	TBC

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description
0.1	IG	2009	Format to Torbay Council
0.2	Andy Booth	2009	Review
0.3	ISG	2012	Review
0.4	Gavin Dunphy	2012	Final review
0.4.1	Gavin Dunphy	2013	Addition of Overseas usage
0.4.2	Kelly Prince	2013	Change in terms
0.4.3	Kelly Prince	2013	Addition of PSN services

1 Purpose

1.1 The purpose of this document is to outline the high level principles that collectively come together to form the Council's Remote Access Policy

1.2 This Remote Access Policy is a key component of Torbay Council's overall information management framework and should be considered alongside more detailed information management and security documentation including: system level security policies; Service Area specific information security guidance and protocols and procedures

1.3 It is intended that by having regard to this policy, as well as related Council wide policies and procedures, and relevant legislation the Council will facilitate not only the protection of its information during processing and transfer of information within the Council; but also compliance with relevant legislation e.g. the UK Data Protection Act, 1998

2 Scope

2.1 This policy applies to all Council staff and Members; to partner agencies and third parties and agents of Torbay Council – where specified by agreement – who have access to information systems, and/or, hold and process information for Torbay Council purposes. It applies to all information assets of the Council, whether or not those assets are managed by the Council.

2.2 Contravention of this policy may lead to disciplinary action, up to and including summary dismissal in very serious cases.

2.3 Remote access is connecting to the corporate computer system by any computer or other electronic device that is not connected to the Corporate Network using the Council wired infrastructure.

The provision of Remote Access and Remote Access Devices must be controlled in order to protect Council systems and data. The controls determine who can access Council systems, how they can access and what can be accessed.

3 Governance factors

Controls on remote connections to the corporate network arise from the rules predefined in the Codes of Connections required to allow Councils to use secure networks.

Remote connections must not be allowed to compromise compliance with a secure network Code of Connection.

4 Remote Access Methods

- Virtual private Network (VPN)
    - This uses an approved client installed on a computer or other electronic device which provides direct encrypted connectivity into the corporate network.

- Thin client (e.g. Citrix)
  - Thin client provides secure remote access via a council hosted web portal. It utilises two factor authentication to prevent unauthorised access.

- Webmail (e.g. Outlook Web Access or OWA)
  - Council provided portal for remote access to corporate mailboxes.

- Third party remote support tools from the internet.
  - This option is not provided by the council; however they are used by some suppliers to provide support.

- Personal Electronic Device (PED) Synchronisation (e.g. Smartphone, Tablet)
  - Council supplied mobile device for synchronising email, calendar and other systems

5 Use of Remote Access methods

The methods of remote access are only to be used in the following circumstances.

- VPN
  - Approved Members and Staff whilst out of the office using council supplied equipment
  - Suppliers to provide remote administration on systems.

- Thin Client (e.g. Citrix)
  - To enable agile working
  - Access to systems and files whilst out of the office.
  - Suppliers to provide remote administration on systems.
  - Third parties requiring access to Council systems.

- Web mail (e.g. OWA)
  - To enable agile working.

- Remote Access web tools
  - Essential support for systems that cannot be provided by other means.

- Mobile Email
  - Members and Staff using Council supplied and approved, smartphones, tablets and PDA's for Council email.

6 Usage Restrictions

- VPN
  - VPN is only enabled using approved software installed by Torbay Council IT Services.
  - On supplier computers, used to provide remote administration on systems, VPN is only enabled using approved software and only gives access to the system being supported.

- Citrix
  - Users must satisfy an approval process.
  - Each approved user will be given a token to provide two-factor authentication.
  - Tokens are not to be shared
  - Tokens assigned to suppliers providing remote support are to be kept with the Council.
  - Citrix Remote Administration procedures must be followed.
  - Once the requirement for Citrix access has finished, the token must be returned to Torbay Council IT Services.

- Outlook Web Access (OWA)
  - Provided to all Members and Council staff who have access to email
  - Removed from generic, Application and non Council staff accounts. Removed from GCSX accounts
  - All temporary files to be cleared after use.
  - Data accessed via OWA must not be saved onto non Council managed devices.

- Remote Access web support
  - Access to Remote Web support websites must be individually approved.
  - Remote access sessions initiated by the supplier must have the support session start logged by Torbay Council IT Services before continuing.
  - Access must only be allowed when all applications apart from the supported application have been closed.
  - All files transferred to the corporate network in order to facilitate the connection must be removed when the session is finished.
  - The supplier must inform Torbay Council IT Services when the session has finished.

- PED Synchronisation
  - Only provided to Members and Council staff who require access to off line email and other Council approved systems. Council managed devices must have encryption,
  - firewall and other security features enabled as deemed necessary for CoCo compliance
  - Device lock must be enabled
  - Device must be stored securely
  - Device must never be left unattended in a public place

7 Remote Administration

- Staff must be individually authorised.
- Suppliers must name the individuals provided with access.
- Each individual person must verify their identity.
- To verify their identity, each named individual will register the answers to secure questions, which will be asked before activation (unless individual known).

- Suppliers must only have support sessions activated by Torbay Council IT Services.
- Suppliers must inform Torbay Council IT Services when the session has finished.

8 Methods of compliance with the controls

- Torbay Council IT Services will provide procedures to control remote access which must be followed by all those using any method of remote access.
- Members or Staff must initiate a security incident report if there is any actual or attempted remote access to the Council corporate system that has not been approved, or may compromise a code of connection to a secure network. This should be reported to IT Services.
- Torbay Council IT Services service desk (01803 207447 or servicedesk@torbay.gov.uk) must be informed immediately (or as soon as possible where access to communication is not available) upon loss / theft of device used to remotely access Council systems.

9 Overseas use

- Council systems should not be accessed from overseas without prior approval of a line manager.
- Council devices (laptops, phones, memory sticks etc) should not be taken overseas without prior approval of a line manager.
- Staff must be alert to the increased risk of theft or loss while travelling. Also, that theft or loss while abroad must still be reported immediately and should not wait until return to the UK.

10 PSN (Public Services Network) Services

Access to any PSN based service is only allowed from devices which are owned and managed by the council. These services include DWP's Customer Information System (CIS) and Tell-Us-Once (TUO).

11 Review of the Resource Protection Policy

11.1 This policy will be reviewed on an annual basis by Information Security Group to ensure that any national or local guidelines, standards or best practices that have been issued and that the Council needs to work to are reflected in the policy in a timely manner.

11.2 Substantive amendment to the policy will be put before the Information Governance forum for comment and adoption. Non-substantive amendments will be actioned and the revised document published in the normal course of business.

11.3 All proposed amendment to the policy will be approved by the Information Security Group.