U04a

Partner Agencies
&
Third Party IT Policy

Target Audience:
Manager

Contents

Document Control

Organisation	Torbay Council
Title	
Creator	Andy Margetts – Operations Manager
Source	Partner Agencies & 3rd Party IT Policy(Torbay Council)
Approvals	
Distribution	
Filename	
Owner	Torbay IT Services / Torbay Information Governance
Subject	Partner Agencies & 3rd Party IT
Protective Marking	
Review date	TBC

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description
0.1	Andy Margetts	2013	Amend to Council
0.2	IS Group	2013	Review
1.0	Kelly Prince	2014	Formatted to Torbay Council

1 Statement of Purpose

The purpose of this document is to outline the high level principles that collectively come together to form the Council's Partner Agencies and 3rd Party IT Policy

This Partner Agencies and 3rd Party IT 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

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 of the Policy

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.

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

3 Key Messages

Partner agencies or 3rd Party suppliers must not be given details of how to access the Council's network or applications without a new starter form (IT05) being completed by the responsible Torbay manager. The new user must be set up as a temporary worker with a maximum of a 12 month period. Any changes to supplier's connections must be immediately sent to the Torbay ICT Servicedesk so that access can be updated or ceased. All permissions and access methods must be controlled via the Torbay ICT Servicedesk.
Partners and 3rd Party suppliers must comply with Torbay's Councils policies before attempting to connect to the Council's network.

The overall security of the Council's ICT infrastructure takes precedence over any individual requirement for access capability.

In order to maintain the confidentiality, integrity and availability of the Torbay Council network, a Code of Connection (CoCo) is required to define the minimum security requirements for any connection to the Council's internal ICT systems from 3rd Party or partner agency staff networks audited by any external organisation.

This policy applies to all 3rd Party organisations that are not already subject to an equivalent or higher Security Classification CoCo that requires site to site

connectivity to the Council's systems. Such access includes temporary connections as well as permanent. The policy covers all possible connection types.

It is the responsibility of the Business Unit Manager to ensure that the 3rd parties they sponsor adhere to ICT Standards in a similar fashion to a Torbay Council employee and to ensure that all reasonable steps are taken to ensure that the confidentiality, integrity and availability of the Torbay Council data and its network is maintained.

Such responsibilities include

- Ensuring anti-virus software is running and up to date.
- Access passwords are protected and are never divulged to anyone else.
- Screen saver programs must be activated and password protected.
- Remote access connections are closed when not in use.
- Applying appropriate protection to any information downloaded from the Councils ICT systems (for example encrypting local copies of sensitive files).

No 3rd Party will be granted access to the network until they have been made aware and formally accepted these responsibilities.

4 Responsibilities for the Torbay Council Business Unit Manager

The Business Unit Managers will ensure that the Torbay Council **IT05** New User & Systems enrolment form is completed before access is granted.
All Business Unit Managers will be responsible for all access provided to 3rd parties under their full or part control. Where the 3rd Party requires access to applications in more than one area of the Council's business, these responsibilities will be shared by the appropriate Business Unit Managers.

Business Unit Managers are responsible for any event that compromises the security (confidentiality, integrity and availability) of any of the Council's ICT systems, networks and data as well as the impact any such event has on the Council, a Council employee or member of the public as a result of the deliberate or accidental misuse of the connection except in cases where the ICT Services Division have failed to implement security controls that are deemed to be reasonable in terms of cost and administrative overhead and within the context of a Local Authority.

The Business Unit Manager will appoint a Point of Contact at the Council with administrative responsibility for the remote access provision. The Point of Contact must liaise with the ICT Services Division and nominated Points of Contacts at 3rd Party sites.

5 Responsibilities of Third Party Organisations

A Primary Point of Contact will be assigned and given the responsibility for managing all aspects of the access provision at the 3rd Party site.

Primary Point of Contact is responsible for providing accurate information about individuals within their organisation with the rights to access Council systems.

The Point of Contact will ensure that all users from the 3rd Party site have received appropriate training or instruction on how to secure the access capability.

The Point of Contact will be responsible for ensuring that the Torbay ICT ServiceDesk is informed when an access connection under their control is no longer required.

The Point of Contact will promptly report any security incident to the Torbay ICT ServiceDesk that may impact upon the confidentiality, integrity or availability of Torbay services & data.

The 3rd Party is responsible for ensuring that all data relating to the function provided to Torbay Council is held and processed only within the EU legislative geographical area, and will be able to provide guarantees and records where applicable to support this.

The 3rd Party will be responsible for any resource or financial implications of implementing this policy.

6 Responsibilities for the ICT Services

It is the responsibility of the ICT Services Division to ensure that access connections are activated and deactivated in accordance with this policy.

7 Remote Access Authorisation

The remote access connections are created for a specific business purpose that is defined by the Information Asset Owner. The remote access connection cannot be used for any purpose other than the intended use.

The Council may enter an agreement with a 3rd Party that effectively allows a group of individuals from that organisation access to the Torbay Council systems and networks. In granting access to such individuals, it is the responsibility of the 3rd Party organisation to ensure that all of the following conditions are met

- The individual has been approved for access by the relevant Torbay Council Business Unit Manager.
- Rights to access the Council network are revoked for that user when such access is no longer required or in cases where the Council decline approval or revoke access rights for that user.
- Third parties agree to communicate the requirements of this policy to its users.
- The User(s) are made aware of the Council's Computer Security Policy
- Where appropriate, third parties may be required to conform to additional Torbay Council Corporate policies. In such cases, a copy of this policy will be provided.

8 Securing Remote Access Connections

All 3rd Parties connecting to the Council network must connect using Council-approved remote access mechanisms; normally a firewalled, authenticated & encrypted method.

3rd Parties must put controls in place to protect Torbay Council from all other networks they may be connected to.

The Council does not support remote access connections from 3rd Parties that originate from dynamic IP addresses. The Council requires all 3rd Party users to connect to the Council's network over statically assigned IP addresses, officially designated connection end point.

9 Connection Monitoring

Remote access connections may be subject to monitoring to include details such as (but not limited to) connection start/stop date and time, user ID, station IDs and authentication method.

The Council reserves the right to audit the 3rd Party site remote access is provided to and any other sites it is logically connected to. Audits may require access to log records, configuration files, systems or other equipment owned by the 3rd Party. Any audit that results in service outage must be agreed in advance.

Monitoring of the remote access is subject to legislation such as the Regulation of Investigatory Powers ACT (RIPA) 2000 and any other legislation covering this activity.

10 Policy Updates

The ICT Services Division reserves the right to make changes to this policy at any time. All stakeholders will be informed of the changes. Business Unit Managers or Third Parties have 30 days to lodge concerns/appeals to the ICT Services Division after which time, the new Policy comes into effect.

11 Non-compliance

The ICT Services Division reserves the right to withdraw the remote access connection without warning where such connections are deemed to threaten the confidentiality, integrity and availability of Council systems.

Serious breaches of this policy may lead early contract termination, civil or criminal action being taken against an individual or organisation

12 Review of the Third Party and Partner Agency Policy

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.

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.

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