Corporate Policy for Third Party Support

1. Introduction

The purpose of this policy is to define standards for all Third Parties seeking to access the Authorities network or any devices attached to the network. This policy is designed to minimise the potential exposure to the Authority and from risks associated with Third Party Access.

2. Objectives of the Policy

The objectives of the policy are

- to improve overall network security
- to prevent unauthorised access
- to protect the Authorities Systems and Data

It must be recognized that this policy is set for the organizations benefit and that there may be occasions when access will be refused / denied if the third party does not adhere to the this policy.

3. Scope of the Policy

This policy applies to all third party users requiring access to the Authorities ICT Network and infrastructure - both internal and external. More specifically this includes

- Individuals, contractors, organisations and system suppliers who do not work for the Authority, but require access to the Authorities network, data or devices, over and above, that of an application user.
- Systems Administrators and Managers organising third party access.
- Where third party individuals are required to gain access to systems as a 'user', they will be required to adhere to the Corporate Acceptable Use Policy.
- Third party access to the Authorities network may be made for administrative, support purposes or to access the third party's own resources electronically

4. Policy

4.1 ***Permitted Third Party Access***

Third party access to the Authorities network / systems may be made for administrative, or support purposes. Third parties wishing to gain access for user functionality will be subject to the Corporate Acceptable Use Policy.

The third party will only be given access to their own systems / folders and not areas for which they do not provide support.

4.2 **Method of Access**

Third parties will be provided with access using two factor authentication key fobs. The specific method of access will depend upon level of service being delivered

- Managed Service – A key fob will be allocated to the third party which they will retain and manage.
- System Support – A specific key fob / user account that will allow access to application, executables and config files. The key fob will remain with ICT / Steria.

4.3 Third Party Access Setup

Third Party Access will only be provided at the request of the service areas Systems Administrator (following completion of appendix 3) or agreed during the installation of a new system. Appendix 3 MUST be completed and signed before Remote Access will be provided. The third party will then be supplied with a username, password and PIN number (these will be required to gain access to the Council's Network).

4.4 Access Requests

Managed Service
Any third party providing a managed service will be able to access servers / systems within scope of that contract. An appropriate contract will define the scope of access required and be approved by the ICT Manager during the procurement process.

System and Application Support
Requests to Access the Council's Network for System or Application Support are managed through the on site Steria Team. Requests to allow access are made as follows.

- Steria will have been notified of the request for access (via Change or Service call) / or made the request for access on behalf of the user).
- The third party will contact the on site team for the six digit code (site specific numbers **Appendix 2 – Third Party Instructions**)
- The engineer will provide the third party with the code but no other information. If the third party does not have a username, password or PIN. Then the third party will need to contact ICT for re-issue of details. Note this will require approval by the Systems Administrator and be provided to the Named Contact only.

Appendix 1 – Agreement

Introduction

The purpose of this contract is to agree conditions for third party access to the Authorities data network.

Third party access is defined as all remote access to the Authorities Data Network or devices attached to the Authorities Network for any purpose.

Access Request

The requester (Council nominated Systems Administrator) has agreed to sponsor the third party Company/individual.

Security Conditions

- Access to Authorities systems and data is granted for approved purposes only. The use of this access for personal use or gain is strictly prohibited.
- Access to the Authorities network facilities will not be provided until a signed copy of this contract has been returned to the Service Desk.
- Authorities network access is limited to the facilities, services and data and connection types as defined in section 4
- The third Party is required to maintain a list of all individuals authorised to use the access and make this available to the Authority on request.
- The third Party must comply with all relevant government legislation including but not limited to the Data Protection Act.
- The Authority reserves the right to monitor activity and revoke access.
- The Authority reserves the right to audit contractual responsibilities.
- Where the third Party has direct or indirect access to data or information owned by the Authority, this information must not be copied, divulged or distributed to any other party.
- On the completion of this contract the third Party must return or destroy all data belonging to Authorities.
- Any suspected security breaches or other incidents must be reported in a timely manner to the Authorities IT Service Desk (08000 288 073)
- The third Party will at all times be held responsible for any activities which occur on Authorities network and applications using any unique user-ids granted.

- The third Party is solely responsible for ensuring that any username(s) and password(s) that they are granted remain confidential and is not used by unauthorised individuals.

- When a third Party is connected to the Authorities network they should not leave the machine/device unattended.

- Workstations/laptops that are used to display Authorities data should be located in such a way that confidential information is not displayed to unauthorised persons or the general public.

- The Authority reserves the right to increase security thresholds if future security risks are identified.

- Normal remote access hours will be 08:00 – 17.30 Monday to Friday.

- All hosts connect to the Authorities networks must: use the most up-to-date anti-virus/anti-spyware/anti-malware software. Be protected by a Corporate or private Firewall. Be up to date with operating system patches. Not be made available for use to unauthorised third parties.

Appendix 2 – Third Party Instructions

System Support

Third parties requiring access are provided with the Username, Password, and User PIN.

- When access is required, you should prepare by connecting to the Citrix Access Gateway Website
  - **HINCKLEY & BOSWORTH BOROUGH COUNCIL:** https://access.hinckley-bosworth.gov.uk
  - **OADBY & WIGSTON DISTRICT COUNCIL:** https://access.hinckley-bosworth.gov.uk
  - **BLABY DISTRICT COUNCIL:** https://access.hinckley-bosworth.gov.uk
  - **MELTON BOROUGH COUNCIL** https://gateway.melton.gov.uk
  - – only supported through Internet Explorer.

- If you have not connected before Download and install the client as prompted.

- Navigate to the appropriate web page, run the security check when prompted and then populate the username and password and domain.

- Call the ICT department for the current code number on the Key Fob.
  - **HINCKLEY & BOSWORTH BOROUGH COUNCIL:** 01455 255 615
  - **OADBY & WIGSTON DISTRICT COUNCIL:** 0116 2572 815
  - **BLABY DISTRICT COUNCIL:** 0116 272 7712
  - **MELTON BOROUGH COUNCIL** 01664 504280 / 2457

- Enter the PIN and this code to complete the login process.

- Select the appropriate desktop.

Managed Services

See Standard Remote Access Document.

This page is intentionally blank – please do not delete as it allows the following form to be removed from the document.

Access Details

Access is granted to	Specify Name and Contact details of Company/Individual including telephone number	
Access is granted to:	Specify System	
Remote access method granted will be	Managed Service Or System Support	

Signed for on behalf of 3rd PARTY

By: _____

Name: _____

Title: _____

Date: _____

Signed for on behalf of Requestor (nominated Council Systems Administrator)

By: _____

Name: _____

Title: _____

Date: _____