Security Incident Procedure

1. Introduction

This procedure describes how security incidents should be dealt with by ICT Staff. The procedure describes the process, category and reporting mechanism.

2. Purpose of the Procedure

The purpose of this procedure is to provide a framework to assist in the investigation of a security incident, and to minimise the operational and financial impact. In the event of an incident, this procedure will establish a chain of command that will set into motion a number of activities to be performed by various staff members internally and externally by partner organisations and individual third-party support agreements.

3. Scope of the Plan

This procedure applies to ICT Personnel and Authority Managers, and describes actions that will be taken in the event of a reported or suspected security incident.

This procedure can operate within wider ICT Policies, Plans and Procedures for example the Disaster Recovery Plan, Discipline and Grievance Policy etc.

The subject of the incident may be any member of Staff, contractor or third party who accesses any of the Shared Service Network and Systems.

4. Response

Following a reported security incident the ICT Manager (or nominated deputy) should be notified immediately, all incident or suspected incidents **must** be reported.. An incident may be received from a line manager, investigation officer, HR, Steria Helpdesk or on-site engineers. Should an individual be unhappy about consulting the ICT Manager then the incident can be raised through the Authory's responsible Director or HR.

The ICT Manager will then make an initial assessment of the situation before constituting the investigation team. The Security Investigation Team will meet to discuss and plan the investigation, identifying key areas of co-ordination and responsibility. The following list is aimed to provide guidance at a generic level:

- Establish the security risk
- Gather Audit Information, Security Logs, Email records
- Alert third-party suppliers should specialist assistance be required
- Establish action plan, assigning clear roles and responsibilities
- Establish Central Help Desk contact for information dissemination
- Alert all IT Services staff to be on standby
- Establish reporting protocols (time and place)
- Establish communication protocols
- Remind staff that direct statements to the media are not to be made. Any media contact is to be made via Council's Communications Officer.

In addition to the above mentioned responsibilities, depending on the nature of the incident, ICT Service staff may be required to report directly to investigating officers, HR or senior managers.

All security incidents will be notified to the Senior Information Risk Officer.

5 Security Risk Classification

In all security incidents – the integrity of the Authority and its systems will be paramount. The Shared Service is a multi-site organisation, which is geographically dispersed. The probability of all sites being affected at the same time is highly unlikely, however, any disruption to a Data Centre will disrupt all that Authority users.

Incidents to ICT Services can be divided into four categories:

Major – A major Security Incident describes situations where the security breach has caused, or will potentially cause loss of service to the major ICT Infrastructure. This includes for example virus attacks, denial of service, hacking. In these situations ICT may decide to make systems un available in order to protect the authority. Generally a major incident would affect the network infrastructure rather than individual systems.

Significant – A significant Incident is one that is constrained to a single application, service or system. Where the removal of the service is sufficient to prevent spread. An example would be where the incident occurred on a sign system, ie the web site.

Minor – A minor incident is one were the breach occurs on an individual basis. For example misuse of email, virus on a stand alone laptop etc. In this instance systems would remain running although ICT Staff may be required to access email accounts, files, folders etc.

Insignificant – An insignificant incident is one that can be tackled before escalating to a higher category. For example a phishing email reported to Steria / ICT Manager before replying, a virus being caught by the anti virus protection etc. In these incidents can be dealt with before causing a problem. These should still be reported to ICT / Steria so that advisory information can be issued to all users.

6. Incident Report

In the event of a security incident a report will be produced detailing the effect of the incident, the cause, action taken and recommendation. The template for this report is shown in Appendix A.

7. GovCertUK

GovCertUK provides CESG's CERT function to UK government. They assist public sector organisations in the response to computer security incidents and provide advice to reduce exposure to threat.

Incidents categorised as Major or significant should be reported to GovCertUK and PSN Security Manager. See www.govcertuk.gov.uk or telephone 01242 709311 for an initial response.

Appendix A – Security Incident Report

POL 019a

RESTRICTED

POL019a

HBBC System Security Incident Report Form

Date/Time of Incident	
Systems Affected	
Details of Incident / Investigation required.	
Actions Taken by ICT	
Recommendations / Findings	
I authorise ICT to undertake the investigations described above and I confirm that I have the necessary authority to make this request.	
Signed (Head of Service)	
Date	