

Information Security Incident Response Procedure

Name: Information Security Incident Response Procedure

Version: 1.5

Issue Date: 05/10/2005



File	Information Security Incident Response Procedure	Pages	1	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Document Control

This is a CONTROLLED document and updates or changes to this document are authorized and then advised by email to the relevant document holders.

It is UNCONTROLLED when printed. You should verify that you have the most current issue.

DOCUMENT HISTORY

Author(s)

Names	Role
John Pritchard	ICT Enterprise Architecture Manager

Document Log

Version	Status	Date Issued	Description of Change	Pages affected	Review
0.9	Draft			All	
1.0	Working	05/10/2005		All	November 2007
1.1	Final	22/01/2008	Updated & Reviewed	All	October 2008
1.2	Final	20/10/2008	Updated & Reviewed	All	October 2009
1.3	Final	11/10/2009	Updated & Reviewed	All	October 2010
1.4	Final	11/05/2010	Removed ISO9001 logo	1	April 2011
1.5	Final	15/06/2011	Reviewed	All	May 2012

File	Information Security Incident Response Procedure	Pages	2	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Contents

<i>1.0 Introduction</i>	4
<i>1.1 What is Information?</i>	4
1.2 What is the Security Approach?.....	4
<i>2.0 Scope</i>	4
<i>3.0 Computer Incident Response Procedure</i>	5
3.1 Incident Classification	5
3.2 Responding to Incidents	6
3.3 Identification	6
3.4 Containment	7
3.5 Eradication.....	7
3.6 Recovery	7
3.7 Follow-up	7
<i>4.0 Enforcement Monitoring</i>	7
4.1 Penalties for Non-compliance.....	8
4.2 Enforcement	8
4.3 Exceptions to the Information Security Policy	8
4.4 Non-compliance.....	9
<u><i>Incident Reporting Process</i></u>	10
Introduction	10
Herefordshire Council ICT Information Security Reporting Procedure.....	11

File	Information Security Incident Response Procedure	Pages	3	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

1.0 Introduction

Information is a valuable asset and is an essential requirement for a local authority to carry out its legal and statutory functions. The information Herefordshire Council processes is about you, it can be highly confidential and very personal; therefore the Authority has a legal duty to take due care of it. This document will address why the Authority needs to secure the information we process, identify the security measures required and provide guidance to users of Authority information.

1.1 What is Information?

Information can be in a number of forms: -

- Spoken in conversations (including telephone)
- Printed out and or written on paper
- Sent by fax
- Sent via E-mail
- Sent by text (SMS)
- Stored on computers
- Transmitted across networks
- Stored on media (tapes, disks, CD's, film, microfiche etc.)
- Stored in databases
- As part of presentations
- Any other methods used to convey information and knowledge.

1.2 What is the Security Approach?

We are obliged by law to deal with any serious breach of information security under the P.A.C.E. (Police And Criminal Evidence) process. The most effective way of providing information security is to use a structured approach that will ensure the appropriate controls are applied to specific areas rather than general controls to all areas. The "Code of Practice for Information Security Management" was published in 1995 as British Standard, BS 7799 (Now ISO27001). This standard provides a comprehensive set of security controls comprising the best information security practices in current use. Its objectives are to provide organisations with a common basis for providing information security and to enable information to be shared between organisations.

2.0 Scope

The Information Security Policy applies to all Herefordshire Council's systems and is effective from the date of issue of this document. The policy, rules and conditions apply to all Herefordshire Council Members, employees, contractors, consultants, agency staff, independent contractors and other users of Herefordshire Council information systems irrespective of the platforms used or where they are located.

File	Information Security Incident Response Procedure	Pages	4	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

3.0 Computer Incident Response Procedure

This document outlines the procedures and responsibilities to ensure quick, effective and orderly responses to security incidents. The purpose of this incident response procedure is to help the Authority quickly and efficiently identify and / or recover from security incidents. The procedure will ensure the minimising of loss, theft, or disruption of critical information services when incidents occur. The term “incident” refers to an adverse event in an information system and/or network or the threat of the occurrence of such an event. The term “incident” encompasses the following general categories of adverse events:

- Inappropriate access level
- Malicious code attacks
- Unauthorised access
- Unauthorised use of information
- Unauthorised utilisation of services
- Disruption of service.
- Misuse
- Espionage
- Hoaxes

An “event” is any observable occurrence in a system or network.

3.1 Incident Classification

Once a security incident is reported, the ICT Information Security Engineer must classify the incident as follows:

“**High**” risk incidents pose a severe risk to Herefordshire Council information and will be classified as critical security incidents. These incidents include, for example, a widespread risk of compromising systems or compromising sensitive or critical data

“**Medium**” risk incidents pose a medium risk to Authority information and as such will be classified as medium-severity security incidents. These incidents include, for example, compromising an information system that does not contain sensitive data and will not pose a widespread risk to other Authority information systems.

“**Low**” risk incidents pose a low risk to Authority information and will be classified as low-severity security incidents. These incidents include, for example, compromise of a system that does not contain critical or sensitive data or pose the risk of compromising other systems.

Incidents will then be dealt with as follows:

“**High**”:

- Isolate the system and remove it from the network as soon as possible
- A Response Time Window of one (1) working hour will be imposed (between 8am and 6pm Monday to Friday).
- Inform senior management as soon as possible

File	Information Security Incident Response Procedure	Pages	5	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

“Medium”:

- Isolate the system and investigate to see whether a compromise has occurred ASAP.
- A response time window of 4 working hours will be imposed (between 8am and 6pm Monday to Friday).

“Low”:

- Isolate the system and investigate.
- A response time window of 1 working day will be imposed

3.2 Responding to Incidents

There are at least five identifiable stages of response to an information security incident. They include:

- Identification
- Containment
- Eradication
- Recovery
- Follow-up.

3.3 Identification

Identification involves determining whether or not an incident has occurred, and if one has what the nature of the incident is.

Typical indications of security incidents include any or all of the following:

- Accounting discrepancies (e.g. someone notices an 18-minute gap in the accounting log in which no entries whatsoever appear)
- Unsuccessful logon attempts
- Unexplained, new user accounts
- Unexplained, new files or unfamiliar file names
- Unexplained attempts to write to system files or changes in system files
- Unexplained modification or deletion of data
- Denial of service or inability of one or more users to login to an account
- System crashes
- Reduction of system performance
- Unauthorised operation of a program or sniffer device to capture network traffic
- “Door knob rattling” (e.g., use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts)
- Unusual time of usage
- An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user
- Unusual usage patterns

Although no single one of these typical symptoms of security incidents is generally by itself conclusive, observing one or more of these symptoms should prompt you to investigate events more closely.

File	Information Security Incident Response Procedure	Pages	6	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

3.4 Containment

Containment involves limiting the scope and magnitude of an incident. The first critical decision to be made during the containment stage is what to do with critical information and/or computing services. Determine whether sensitive information should be left on information systems or whether it should be copied to media and taken off-line. It may similarly be best to move critical computing services to another Authority information system on another network where there is considerably less chance of interruption.

The next decision concerns the operational status of the compromised system itself. Should this system be shut down entirely, disconnected from the network, or be allowed to continue to run in its normal operational status so that any activity on the system can be monitored? The answer depends on the type and magnitude of the incident. In the case of a simple virus incident, it is almost certainly best to quickly eradicate any viruses without shutting the infected system down. If the system is sensitive, information or critical programs may be at risk, and it is generally best to shut the system down (or at least temporarily disconnect it from the network). If there is a reasonable chance that a perpetrator will be identified, by letting a system continue to run as normal, the Authority must assess and accept the potential risk of damage, disruption, or the compromise of data. Document all containment procedures for Security Forum review and keep senior management informed.

3.5 Eradication

Eradicating an incident entails removing the cause of the incident.

3.6 Recovery

Recovery means restoring a system to its normal status.

3.7 Follow-up

Some incidents require considerable time and effort. Performing follow-up activity is, however, one of the most critical activities in responding to incidents. Following up afterwards will help the Authority improve their incident handling procedures and review their ISMS (information Security Management System) as well as continue to support any efforts to prosecute those who have broken the law. Follow-up activities include the following:

- Analysing what has transpired and what was done to intervene.
- Analysing the cost of the incident.
- Preparing a report for the Security Forum
- Revising the ISMS. "Lessons learned" contained in the report described above should be used as the basis for modifying Authority information incident response policies and procedures.

Once the above incident response procedure has been completed, all information will be logged by the ICT Information Security Engineer for review by the Security Forum. Impact on the ISMS will also be discussed.

4.0 Enforcement Monitoring

Monitoring of the standard is the responsibility of all managers as part of their management role. The Internal and External Audit may undertake reviews on a planned and ad-hoc basis as part of the audit process. The IT Security team will conduct quality reviews on cyclical basis as part of their security role.

File	Information Security Incident Response Procedure	Pages	7	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

4.1 Penalties for Non-compliance

The Authority has an established staff Disciplinary Code of Conduct. Any breach of policies contained within this document will be dealt with in accordance with those procedures.

4.2 Enforcement

A violation of standards, procedures, or guidelines established in support of this policy will be brought to the attention of the ICT Information Security Engineer for investigation. The IT Security Team enforces this policy by continuously monitoring, through the use of software tools. Business Unit Management, Human Resources, Internal Audit and External Audit will be notified when it is considered a breach has taken place. It is the responsibility of all users (as defined within the Scope of this document) to ensure compliance with the policy. Failure to adhere to the policy may result in a breach of Financial Regulations, Standing Orders and or current legislation. In the event of a breach by a Authority employee,, IT facilities may be suspended/removed and disciplinary action taken in accordance with the Disciplinary Code of Conduct. Action against non-Herefordshire council employees may result in removal/suspension of IT facilities, removal from site, cancellation of any contracts and possible legal action.

4.3 Exceptions to the Information Security Policy

The Authority expects all Employees and Members to achieve compliance with the directives presented within this policy. In the following exceptional cases, compliance with the Authority's Information Security policies may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question. These exceptional circumstances are outlined below:

- If complying with the policy would lead to physical harm and/or injury to a member of staff or other third party (e.g. contractor).
- If complying with the policy would cause significant damage to the Authority's reputation and/or ability to operate
- If an emergency arises and a user has no alternative other than to breach Authority policy to assist with the emergency.

In such cases, the Authority employee or third party (contractor etc) concerned must take the following action:

- Ensure that a Manager is made aware of the situation and the action to be taken.
- Ensure the situation and the actions taken are recorded in as much detail as possible
- Ensure the situation is reported to the ICT Information Security Engineer as soon as possible.

(Failure to take these steps may result in disciplinary action).

The ICT Information Security Engineer will:

Maintain a list of known exceptions and non-conformities to the Information Security Policies. This list will contain:

- Known breaches that are in the process of being rectified
- Minor breaches that are not considered to be worth rectifying
- Any situations to which the Information Security Policies are not considered applicable.
- The Authority will not take disciplinary action in relation to known, authorised exceptions to the Information Security Policies.

File	Information Security Incident Response Procedure	Pages	8	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

4.4 Non-compliance

Non-compliance is defined as any one or more of the following:

- A breach of The Authority's Information Security Policies, standards or controls. Unauthorised disclosure or viewing of confidential information belonging to the Authority
- Unauthorised modification to information, software or operating systems
- The use of hardware, software, communication networks, equipment, data or information for illicit purposes, which may include violations of law, regulation or reporting requirement of any enforcement agency or government body
- The exposure of the Authority to adverse publicity or actual or potential monetary loss through any compromise of security
- Any person who knows of, or suspects a breach of the Authority's Information Security Policies must report the facts immediately to the ICT Information Security Engineer or Senior Management, failure to do so will be treated as non-compliance to the Information Security Policy
- Violation or non-compliance with the Authority's Information Security Policy may be treated as gross misconduct.
- Penalties may include:
 - Suspension of system access rights
 - Action in accordance with the Authority Disciplinary Code of Conduct
 - Termination of employment or contractual arrangements and civil or criminal prosecution

File	Information Security Incident Response Procedure	Pages	9	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Incident Reporting Process

Introduction

This document has been created to clearly lay out the process that is undertaken by Herefordshire Council ICT section, when a suspected information security incident is reported or observed.

The first process flowchart:

“Herefordshire Council ICT Information Security Reporting Procedure “ has been laid out in such a way so as to align with the requirements of the International Standard ISO17799, meeting requirement:

A 13.1 Reporting Information Security Events and weaknesses

- **A 13.1 Responding to security incidents and malfunctions** – Objective To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents.
- **A 13.1.1 Reporting security incidents** – Security incidents shall be reported through appropriate management channels as soon as possible after the incident is discovered
- **A 13.1.2 Reporting Security Weakness** – Users of information services shall be required to note and report any observed or suspected security Weaknesses in or threats to systems or services
- **A 13.2.1 Responsibilities & Procedures** - Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

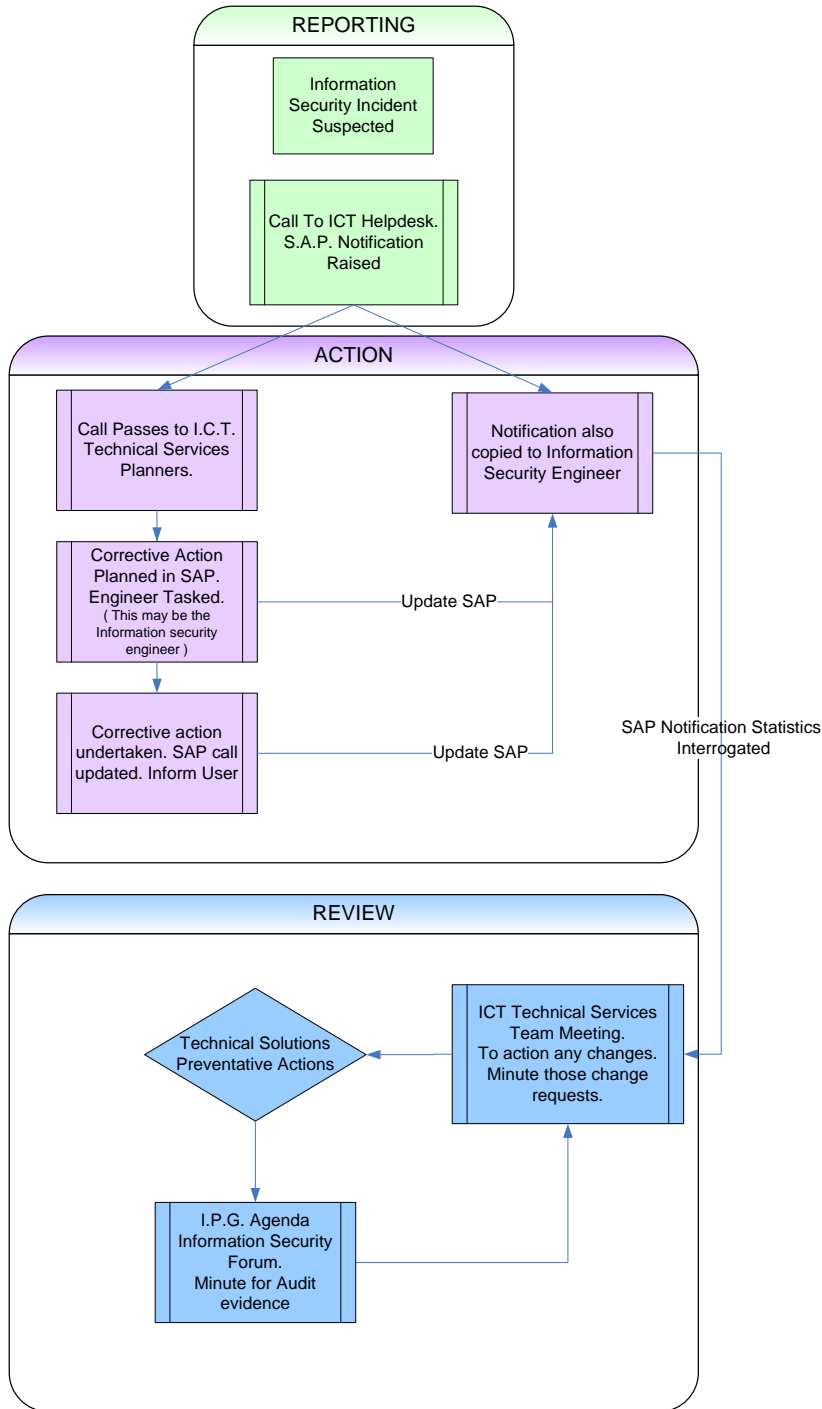
A 13.2 Management of Information Security Incidents and Improvements

- **A 13.2.2 Learning from Information Security Incidents** – There shall be mechanisms in place to enable the types, volumes and costs of information security incidents to be quantified and monitored.
- **A 13.2.3 Collection of Evidence** - Where a follow-up action against a person or organization after an information security incident involves legal action (either Civil or Criminal), evidence shall be collected, retained and presented to conform with the rules for evidence laid down in the relevant jurisdictions

The ability to report a suspected, potential, information security incident should be made available for all Herefordshire Council employees.

File	Information Security Incident Response Procedure	Pages	10	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Herefordshire Council ICT Information Security Reporting Procedure



File	Information Security Incident Response Procedure	Pages	11	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified