



Information Security Document

Security Incident
Management
Policy and Procedures

Version 10.0

Version History			
Version	Date	Detail	Author
1.0	27/10/2010	Completed for Distribution	Jo White
1.0	21/12/2010	Approved by Information Governance Group	Jo White
2.0	22/06/2012	Reviewed by Information Governance Group. Approved by email due to meeting being cancelled.	Jo White
3.0	30/09/2012	Reviewed by Information Governance Group	Jo White
4.0	28/10/2013	Reviewed by Information Governance Group	Jo White
5.0	03/11/2014	Reviewed by Information Governance Group	Jo White
6.0	15/12/2015	Reviewed by Information Governance Group. No changes.	Jo White
7.0	03/04/2017	Reviewed by Information Governance Group. Transformation changed to ICT.	Jo White
8.0	03/04/2018	Reviewed by Information Governance Group. GDPR requirements added.	Jo White
9.0	07/05/2019	Reviewed by Information Governance Group. Dnet reporting form removed.	Jo White.
10.0	16/06/2020	Reviewed by Information Governance Group. Legal obligations updated.	Jo White
This document has been prepared using the following ISO27001:2013 standard controls as reference:			
ISO Control	Description		
A.16.1.2	Reporting Information Security Events		
A.16.1.3	Reporting Information Security Weaknesses		
A.16.1.6	Learning from Information Security Incidents		

1 Introduction

Derbyshire County Council is responsible for the security and integrity of all data it holds. The Council must protect this data using all means necessary by ensuring at all times that any incident which could cause damage to the Council's assets and reputation is prevented and/or minimised. This is particularly important given that the new General Data Protection Regulation (GDPR) and associated legislation gives the relevant regulator, the Information Commissioner, the power to impose very substantial fines on the Council. There are many types of incidents which could affect security:

- A computer security incident is an event which could include but is not limited to:
 - loss of confidentiality of information
 - compromise of integrity of information
 - denial of service
 - unauthorized access to systems
 - misuse of systems or information
 - theft and damage to systems
 - virus attacks
 - intrusion by humans
- Other types of incidents may include:
 - Loss of ID badge/s
 - Missing correspondence
 - Exposure of Uncollected print-outs
 - Misplaced or missing media
 - Inadvertently relaying passwords
 - Loss of mobile phones and portable devices

Ensuring efficient reporting and management of security incidents will help reduce and in many cases, prevent further incidents occurring.

More detailed information on the type and scope of security incidents is provided in the Policy Statement section of this policy.

2 Purpose

The management of security incidents described in this policy requires the Council to have clear guidance, policies and procedures in place. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which often go unreported and unnoticed – sometimes, over a long period of time and often without resolution.

The purpose of this policy is to:

- Outline the types of security incidents
- Detail how incidents can and will be dealt with
- Identify responsibilities for reporting and dealing with incidents
- Detail procedures in place for reporting and processing of incidents
- Provide Guidance

3 Scope

This policy applies to:

- Council employees, elected members, partner agencies, contractors, volunteers and vendors
- All Council departments, personnel and systems (including software) dealing with the storing, retrieval and accessing of data

4 Policy Statement

The Council has a clear incident reporting mechanism in place which details the procedures for the identifying, reporting and recording of security incidents. By continually updating and informing all parties identified within the scope of this policy of the importance of the identification, reporting and action required to address incidents, the Council can continue to be pro-active in addressing these incidents as and when they occur.

All parties identified within the scope of this policy are required to report all incidents – including potential or suspected incidents, as soon as possible via the Council's Incident Reporting procedures.

The types of Incidents which this policy addresses include but is not limited to:

Computers left unlocked when unattended

Users of Council computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All parties identified within the scope of this policy need to ensure they lock their computers appropriately - this must be done despite the fact that Council computers are configured to automatically lock after 10 minutes of idle time. Discovery of an unlocked computer which is unattended must be reported via the Council's Incident Reporting procedures.

Password disclosures

Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedures for authorisation – initially through the individual's line manager. If anyone suspects that their or any other user's password has been disclosed whether intentionally, inadvertently or accidentally, the ICT Service must be notified through the Council's Incident Reporting procedures. For more information, the Council Password policy is available on the intranet (Dnet), main Council website or via the ICT Service's Service Desk. Under no circumstances should an employee allow another employee to use their user account details – even under supervision.

Virus warnings/alerts

All Desktop, laptop and tablet computers in use across the Council have Antivirus (including Anti-Spyware/Malware). For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft or damage to Council data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported by the user to the ICT Service's Service Desk as soon as possible.

V10.0

Derbyshire County Council Security Incident Management Policy and Procedures

Media loss

Use of portable media such as CD/DVD, DAT (magnetic tape), USB Flash sticks/HD drives for storing data requires the user to be fully aware of the responsibilities of using such devices. The use of PCs, laptops, tablets and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorised access. Any authorised user of a portable device (including portable media) who has misplaced or suspects damage, theft whether intentional or accidental must report it immediately through the Council's Incident Reporting procedures.

ID Badges

It is essential for us to identify individuals and wearing ID badges helps us to do this. The following documents detail the use of ID badges and can be found using the following link:

Safe Haven Guidance and Physical and Environmental Infrastructure Procedures:

http://www.derbyshire.gov.uk/working_for_us/data/default.asp

Data loss/disclosure

The potential for data loss does not only apply to portable media it also applies to any data which is:

- Transmitted over a network and reaching an unintended, unauthorised - recipient (such as the use of e-mail to send sensitive data)
- Intercepted over the internet through non secure channels
- Posting of data on the internet whether accidental or intentional
- Published on the Council's website and identified as inaccurate or inappropriate
- Conversationally – information disclosed during conversation
- Press or media – unauthorised disclosure by employees or an ill advised representative to the press or media
- Data which can no longer be located and is unaccounted for on an IT system
- Unlocked and uncollected print-outs from Multi-Function Devices (MFDs)
- Paper copies of data and information which can no longer be located
- Hard copies of information and data accessible from desks and unattended areas

All parties identified within the scope of this policy must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of Council data at all times.

Any loss of data and/or disclosure whether intentional or accidental must be reported immediately using the Council's Incident Reporting procedures

Personal information abuse

All person identifiable information – i.e. information which can identify an individual such as home address, bank account details etc... must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.

Any abuse/misuse of such person identifiable information must be reported through the Council's Incident Reporting procedures.

Physical Security

V10.0

Derbyshire County Council Security Incident Management Policy and Procedures

Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room – e.g. a combination key lock mechanism. Lower / floor level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data - concerns about any rooms/office which should be securely locked or access restricted must be reported to the ICT Service via the Council's Incident Reporting procedures.

Continuing emphasis and re-enforcement of the Council's Secure Desk policy will further help to reduce the number of security incidents.

Logical Security / Access Controls

Controlling, managing and restricting access to the Council's network, databases and applications is an essential part of Information Security. It is necessary to ensure that only authorised employees can gain access to information which is processed and maintained electronically.

Missing correspondence

Data or information which has been sent either electronically or physically which cannot be accounted for e.g. not arrived at the intended destination via physical post, sent electronically, sent for printing but no printed output retrieved etc... must be reported through the Council's Incident Reporting procedures.

Found correspondence/media

Data stored on any storage media or physically printed information which has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access e.g. unlocked printouts, discarded CD (media), must be reported through the Council's Incident Reporting procedures.

Loss or theft of IT/information

Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinet etc... or which is known/or suspected to have been stolen needs to be reported immediately through the Council's Incident Reporting procedures

5 Responsibilities

It is the responsibility for all parties identified within the scope of this policy who undertake work for the Council, on or off the premises, to be proactive in the reporting of security incidents. The Council's Incident Reporting procedures are in place to prevent and minimise the risk of damage to the integrity and security of Council data and information.

It is also a responsibility of all parties identified within the scope of this policy to ensure that all policies and procedures dealing with the security and integrity of information and data are followed.

6 Compliance with legal and contractual obligations

GDPR and the Data Protection Act (2018) requires that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Computer Misuse Act (1990) covers unauthorised access to computer systems.

7 Breaches of Policy

Breaches of this policy and/or security incidents are incidents which could have, or have resulted in, loss or damage to Council assets, including IT equipment and information, or conduct which is in breach of the Council's security procedures and policies.

All parties identified within the scope of this policy have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council. In the case of third party vendors, volunteers, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Council's ICT systems or network results from the non-compliance, the Council will consider legal action against the third party. The Council will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an employee, infringements will be investigated under the disciplinary procedure and progressed as appropriate.

The Council is under a legal obligation to report certain types of breaches to the Information Commissioner's Office (ICO).

Breaches will be reportable to the ICO if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms. Affected individuals will also have to be notified of the breach without undue delay.

Relevant breaches will normally be reportable to the ICO within 72 hours of the loss occurring. It will be the responsibility of the Council Data Protection Officer acting in consultation with the SIRO to decide whether an individual security incident should be reported to the ICO.

This Policy is referenced by other Council policies and guidelines. Copies of these policy statements are obtainable via the Council's Intranet (Dnet) or by request to the ICT Service, as appropriate.

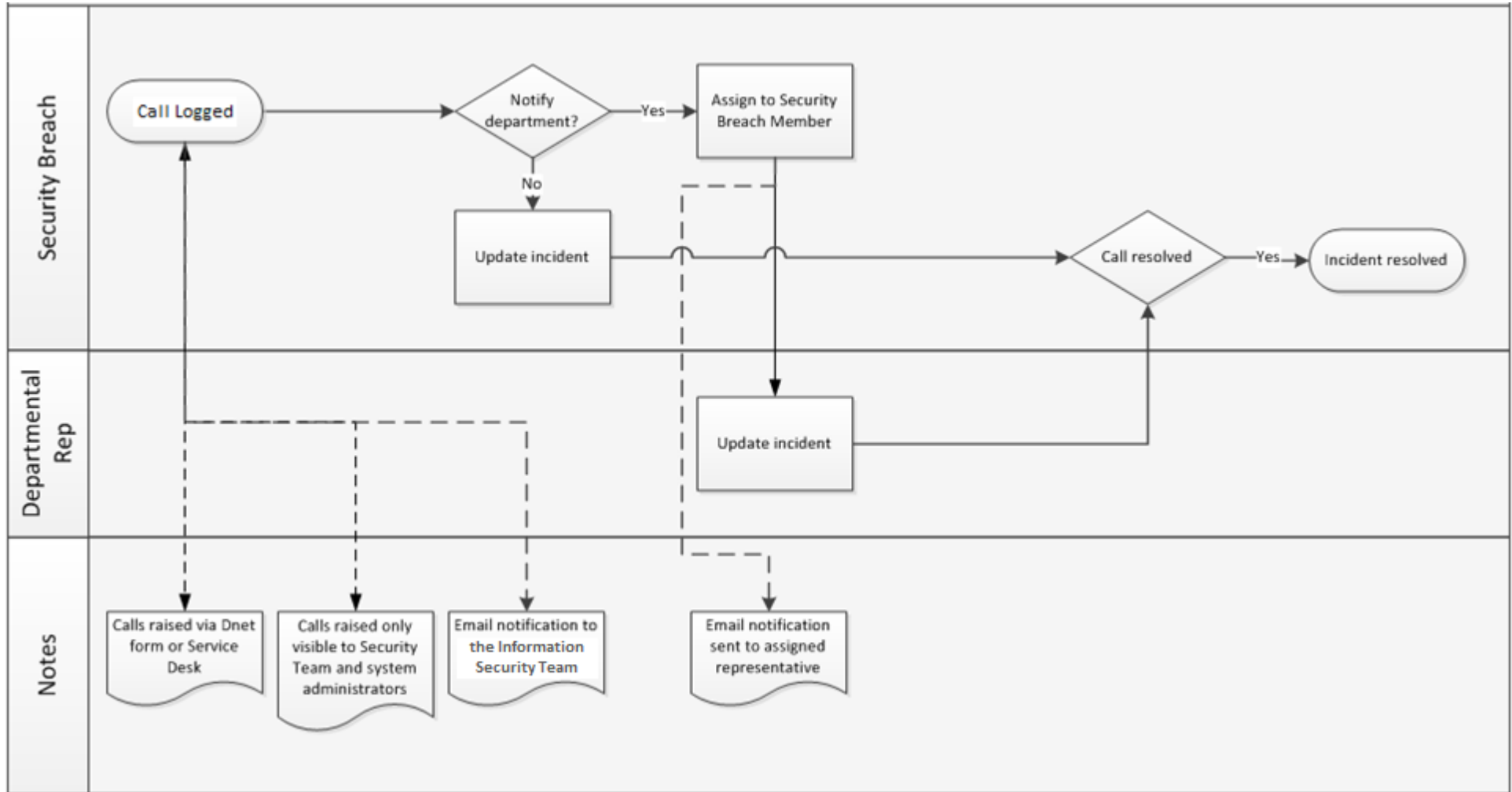
This Policy is maintained and reviewed by the Council's Security/Business Continuity Team and ratified by the Council's Information Governance Group.

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.

Incident Reporting And Management Procedure

PUBLIC

Any incident, as described in the Policy and which needs reporting, will follow the process:



8.0 Overview

The ICT Service will continually highlight the importance of incident reporting and will further encourage the methods by which security breach incidents can be reported. Where computer access to the Council network or Council website is not available, breaches can be reported via a telephone call to the ICT Service's Service Desk. Breaches can involve not only Information Technology equipment but also data that is mishandled, lost or abused or any other incident which may cause a security concern or which may contravene the Council's Safe Haven Guidance and associated policies.

8.1 Incident Reporting

Any breach of the Incident Management Policy must be reported as soon as possible via the reporting procedure. In cases where the confidential reporting procedure may need to be followed, the link below is provided:

http://dnet/policies_and_procedures/corporate_governance/confidential_reporting_code/default.asp

8.2 Methods of reporting:

The following methods can be used to record security incidents:

- Using the Service Desk Online icon on the desktop
- Via a Phone call to the Service Desk
- E-mailing the Service Desk

Reporting via the Service Desk Online desktop icon:



All computer desktops on the Council network have a Service Desk Online icon (as above). Double-clicking on this icon will take you to the incident reporting page:

DERBYSHIRE
County Council
Improving life for local people

Home

Help Articles









My Requests

My Activities







Service Status

Escalation Procedures

1 Password Resets


 AD Account (log onto computer)	 Framework-I	 GCSX Account
 Juniper VPN 3rd Party	 Pitney Bowes Confirm	 SAP
 Total (formerly Task)	 Tribal	

2 General

 Printing & Scanning Requests for printing & scanning functionality	 Report a Fault Log a fault call with the Service Desk	 Request Something New Make a request for something new
 Secure Data Transfer Request relating to Secure Data Transfer	 Security Incidents Report a Security Incident	 Telephony & Connectivity Log a request relating to VoIP phones, Corporate mobile phones & network...

Security incidents can be reported by clicking on the link displayed and providing information on the following:

- Incident Date/Time
- Department – drop down menu
- Work location/site
- Contact details phone etc
- Type of incident – from drop down menu
- Description – more detailed information about the incident

 **Report a Security Incident** [Security Incidents](#)

Incident Date\Time

Select your Department from dropdown list

SELECT YOUR DEPARTMENT FROM THE LIST BELOW

Work Location\Site

Contact Details

Select your Incident Type from list below

SELECT INCIDENT FROM THE LIST BELOW

When a call is logged through the Service Desk Online icon on the desktop or the Dnet form, an e-mail is generated and sent to the Information Security Manager and Head of the ICT Service. The request is logged in the call logging system (Service Manager) and is only visible to the Information Security Manager and Head of the ICT Service.

Reporting via the Service Desk

Security incidents and breaches can be reported by telephoning the ICT Service's Service Desk on 01629 537777.

A Service Desk representative will log the details of the call in the call logging system based on the information given by the caller. Callers are advised to give as much information as possible and should be able to give similar details as required when completing the online form.

The Service Desk representative will log the call and any further progress or information about the incident will be dealt with by the Information Security Manager or nominated departmental representative.

Reporting via E-mail

Security breaches may be reported via e-mail to the ICT Service's Service Desk however, wherever possible, confidential or personal identifiable information should not be contained in the e-mail e.g. logon passwords.

8.3 Incident Management

When an incident is reported and entered into the call logging system, an email is generated and sent to the Information Security Manager and also copied to the Assistant Director of ICT (Operations). The Information Security Manager will then determine if the incident needs to be escalated to the appropriate pre-identified departmental representative to deal with as soon as possible. Representatives looking into security breaches will be responsible for updating, amending and modifying the status of incidents in Service Manager.

All parties dealing with security incidents shall undertake to:

- analyse and establish the cause of the incident and take any necessary steps to prevent recurrence
- report to all affected parties and maintain communication and confidentiality throughout investigation of the incident
- identify problems caused as a result of the incident and to prevent or reduce further impact
- contact 3rd parties to resolve errors/faults in software and to liaise with the relevant ICT Service and departmental personnel to ensure contractual agreements and legal requirements are maintained and to minimise potential disruption to other Council systems and services
- ensure all system logs and records are securely maintained and available to authorised personnel when required
- ensure only authorised personnel have access to systems and data
- ensure all documentation and notes are accurately maintained and recorded in Service Manager and made available to relevant authorised personnel
- ensure all authorised corrective and preventative measures are implemented and monitored for effectiveness

Where appropriate, Incidents will be presented to the Information Governance Group (IGG) meetings via departmental representatives and will be included on the Corrective And Preventative Action (CAPA) log

V10.0

Derbyshire County Council Security Incident Management Policy and Procedures

All incidents logged within Service Manager shall have all the details of the incident recorded – including any action/resolution, links or connections to other known incidents. Incidents which were initially resolved but have recurred will be reopened or a new call referencing the previous one will be created.

Monthly reports on incidents generated by the Service Manager system are automatically sent to the Information Security Manager to facilitate the monitoring of the types, numbers, frequency and severity of incidents which will help to correct and prevent incidents recurring.

During the course of incident investigations, hardware, logs and records may be analysed by the Council's internal Audit function. Information and data may be gathered as evidence to support possible disciplinary or legal action. It is essential during the course of these investigations that confidentiality is maintained at all times.

The Information Security Manager is initially responsible for handling security incidents and will make a decision as to whether an incident needs to be "handed" over and dealt with (including closed) by departmental representatives where appropriate.

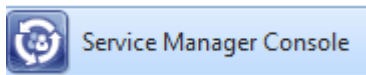
How security incidents are handled by the ICT Service

The information regarding any incident which has been provided will be logged in Service Manager and will create an Incident/Service Request record.

The Service Manager call logging system will generate an email and send it to Information Security Manager and to the Assistant Director of ICT (Operations).

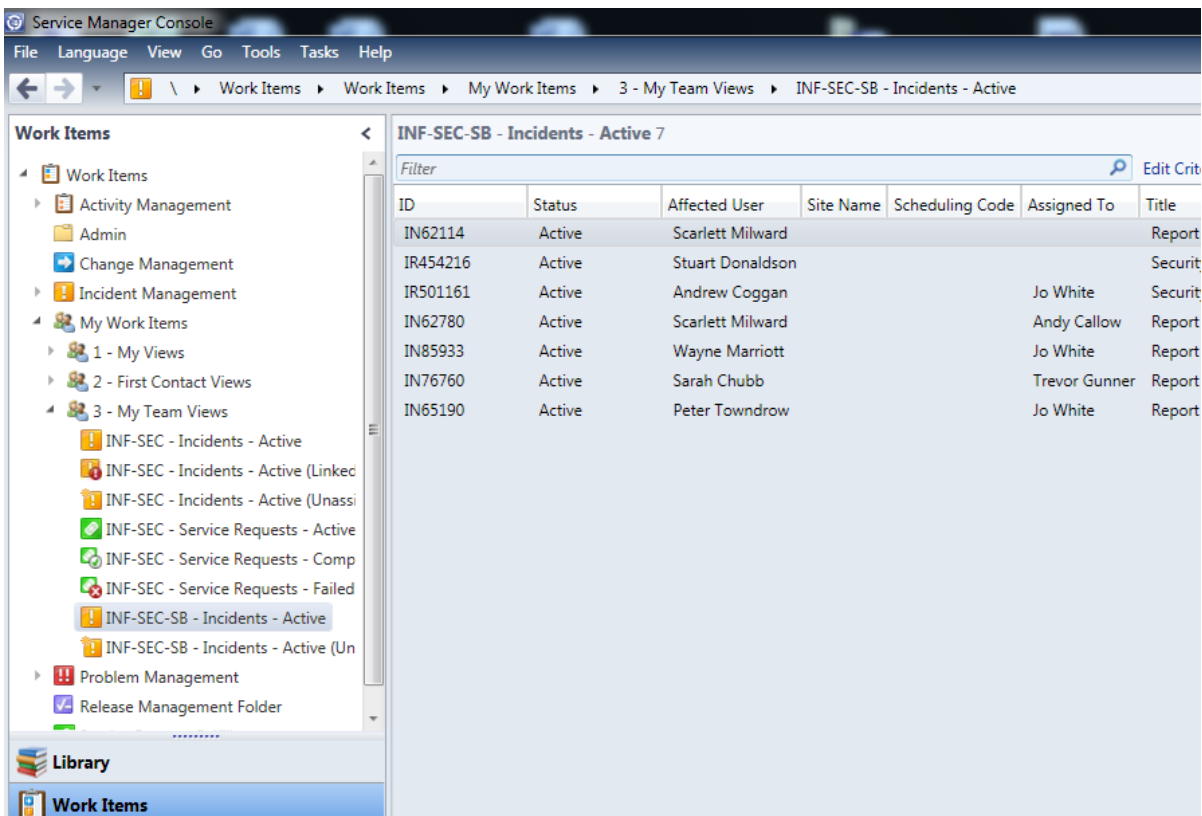
The Information Security Manager will access the logging system (Service Manager) to deal with any reported incidents and will assign the incident to the relevant departmental representative if required.

Access to the Service Manager system is provided using the following shortcut which is made available from the computer start menu:



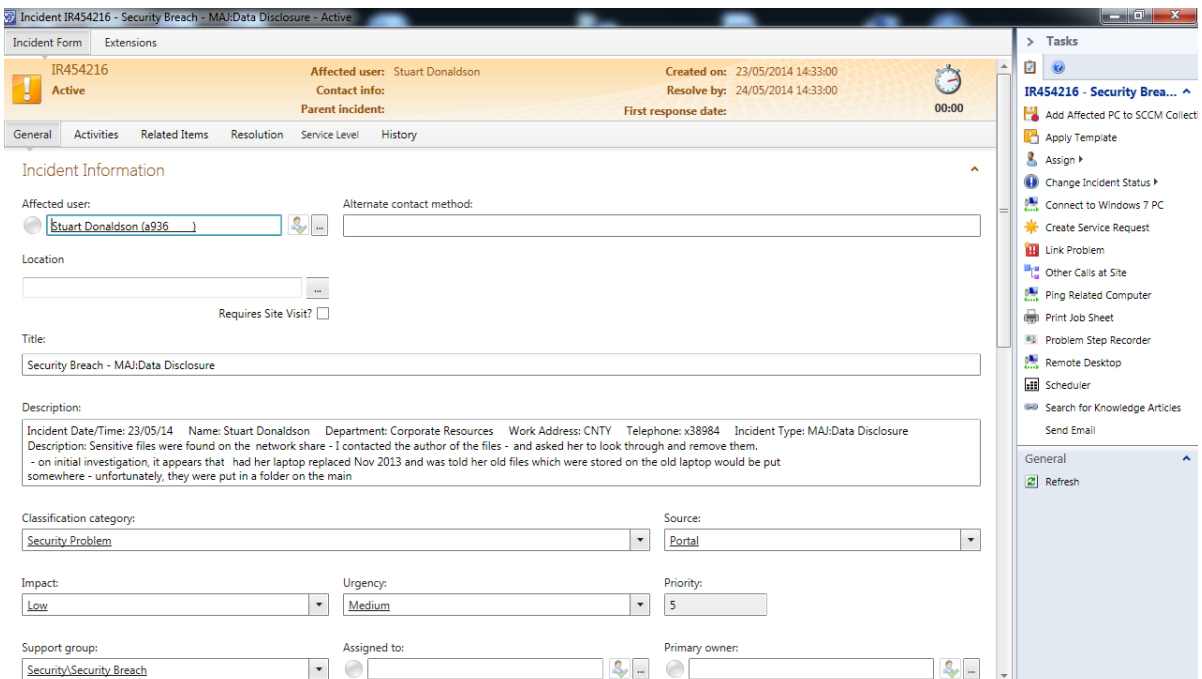
If you have been nominated to deal with security breaches in your department, you will be provided access to the Service Manager Console. If you don't have the Service Manager Console application on your computer, installation can be arranged by contacting the ICT Service's Service Desk on 01629 537777.

The Information Security Manager/security team will be able to see the logged incident in the security team's view within the Service Manager application:



Double-clicking on any incident provides further details which the security team will use to determine how the incident is handled and who should deal with it.

In this screen, the affected user is displayed along with the initial title and description of the incident. You will also notice there are 'drop down' sections which define the incident further.



The following screen displayed shows the continuation of the above screen which provides further information such as comments provided in an 'Action Log':

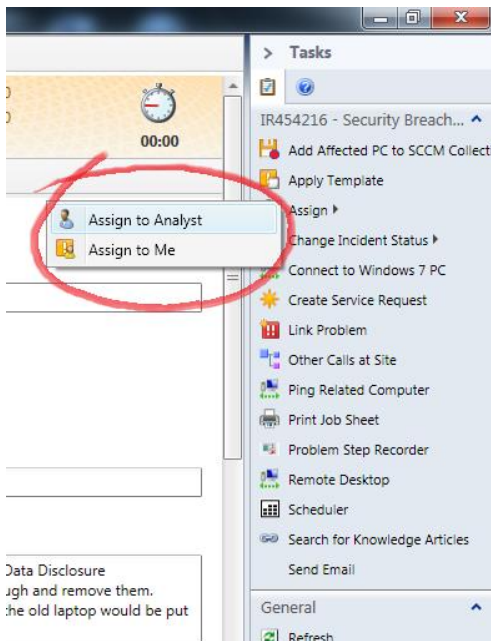
Log entry	Private	Created by	Date time
Analyst Comment	<input type="checkbox"/>	Stuart Donaldson	23/05/2014 14:39:30
Analyst Comment	<input type="checkbox"/>	Stuart Donaldson	23/05/2014 16:31:20
Record Resolved	<input type="checkbox"/>	Stuart Donaldson	26/06/2014 14:18:49

The Information Security Manager will determine whether the incident can be resolved at this point. If the incident can be resolved by the security team, the Information Security Manager will:

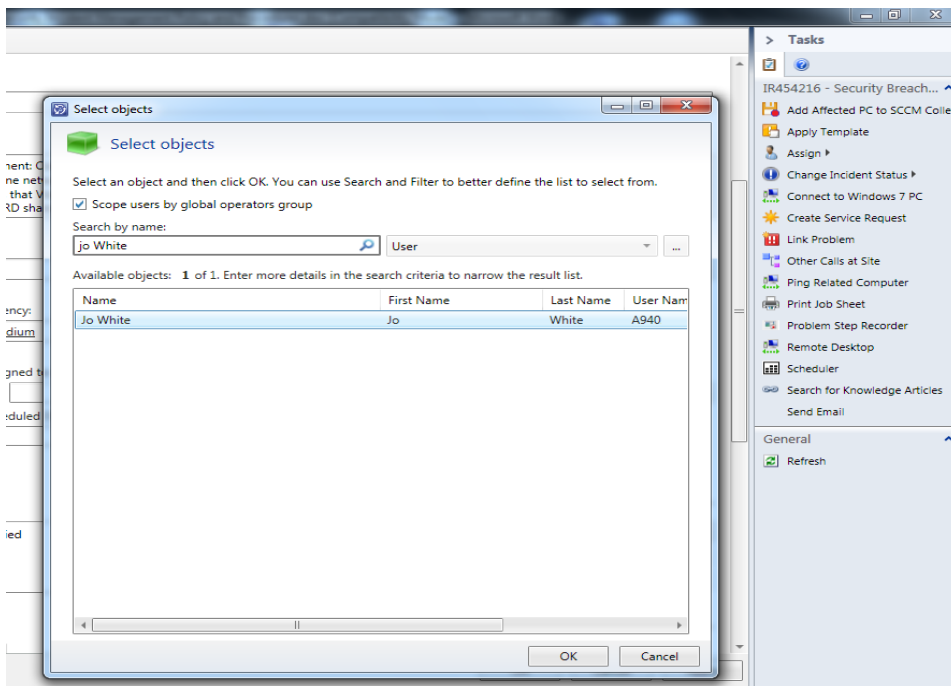
Click on the '**Change Incident Status**' and '**Resolve**' button to the bottom right of the screen and complete the comments in the 'Resolve' window:

After selecting the 'Resolution Category' and completing the comments section (required), clicking on the 'OK' button will set the incident to be 'Closed'

If the Information Security Manager/security team cannot resolve the incident, it will be re-assigned by clicking 'Assign' and 'Assign to Analyst' and selecting the name for the appropriate representative:



Clicking on an appropriate name and clicking 'OK' will assign the incident to that person to deal with:



Please note: an incident must be resolved before being closed

Further information and guidance on the use of Service Manager and the recording of incidents may be obtained by contacting the ICT Service's Service Desk on x37777

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.