Data Breach and Information Security Incident Procedure

Version: 5
Date Issue: May 2018
Review date: April 2020
Reference: WCCC-1073-648
Team: Information Management
Protective Marking: Public

Warwickshire County Council

Working for Warwickshire

Contents

Version history and approvals

V1	Information Governance Steering Group	November 2010
V2	SIRO, Monitoring Officer	October 2011
V3	Information Governance Steering Group	March 2012
V4	Information Governance Steering Group	April 2016
V5	Information Governance Steering Group	May 2018

1. Introduction

Warwickshire County Council (WCC) is committed to the protection of information and has in place a number of technical and organisational measures to safeguard the information it owns. This includes technical security ranging from secure passwords and system encryption, and organisational safeguards ranging from physical building and office security to procedural standards and requirements for the safe handling and storage of information. This procedure covers reporting of actual or suspected data security incidents that may be data breaches.

These procedures are **mandatory** and must be followed by all staff as part of the council's Information Governance Framework the standard for managing information in the council and is one of the linked procedures in the Information Compliance policy aimed at all staff

2. Purpose

The Council recognises that from time to time 'things go wrong' and there may be a breach of security involving information or equipment holding information. The purpose of this procedure is to ensure that all actual or potential information security incidents are reported centrally to enable the Council to react quickly and effectively to minimise the impact.

The aims of the procedure are as follows:

- Timely advice on containment and risk management
- Determine whether further controls or actions are required
- Consider whether the incident is required to be notified to the Information Commissioner's Office (ICO) and/or the NHS, and the individual(s) affected by the incident
- Evaluate lessons learnt and areas for improvement

All information security incidents will be dealt with by the WCC 'Incident Group', which comprises of lawyers from the Council's Corporate Legal Service (Group Members) with a nominated Incident Lead, who will review and advise on incidents and make recommendations on appropriate follow up and corrective action. Specialist input will be sought from the Data Protection Officer, ICT Cyber Security or Information Management where necessary.

3. Scope

This procedure applies to all staff including: employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information.

The Council requires organisations providing services that hold or process personal

information on its behalf (i.e. acting as data processors) to have in place internal reporting requirements equivalent to this procedure and for any third party breaches to be reported immediately to the WCC Data Protection Officer in the first instance.

4. Identifying Incidents

The General Data Protection Regulation (Regulation (EU) 2016/679) defines a data breach as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. Information security incidents can therefore cover a multitude of situations, but generally it will involve an adverse event which results, or has the potential to result in the compromise, misuse or loss of WCC owned or held information or assets. Data breaches can be categorised according to the following three information security principles:

- Confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data
- Availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data
- Integrity breach – where there is an unauthorised or accidental alteration of personal data.

Information in this procedure is used as a collective term and may include personal or sensitive/ special category personal data as defined under the data legislation (or confidential personal data as commonly referred to in the health sector) and also business information.

Some examples of information security incidents include (but are not limited to):

- the loss or theft of information or equipment,
- incorrect handling of protectively marked information,
- poor physical security,
- hacking,
- information disclosed in error,
- unauthorised use or access to information or systems.

The impact of a security incident can vary greatly depending on the type of information or asset involved. It may for instance lead to an infringement of privacy, fraud, financial loss, service disruption or reputational damage. The purpose of reporting an incident is not to apportion blame but to ensure that any impact is minimised and lessons learnt can be identified and disseminated.

The principles of this procedure also apply to cyber incidents i.e. any incident that could or has compromised information assets within the Council’s digital network for e.g. phishing emails or hacking attacks. Any cyber-related incident will be handled in accordance with WCC’s Cybersecurity Incident Response Procedure in Appendix D by the Cyber Security Incident Response Team (CERT).

In the event that a cyber incident also involves a data breach then it shall remain subject to

this procedure and the Incident Lead (or Group Member) will work in conjunction with the CERT Team to resolve the incident and report to regulators as necessary.

5. Reporting Incidents

A direct line manager or supervisor should always be made aware of any information security incident and the incident reported in line with this procedure. Informing a line manager or supervisor of an incident must not delay any incident being reported under this procedure.

All information security incidents should be reported immediately (and in any event within 4 hours) after an individual is aware of a potential or actual incident. Informing a line manager or supervisor of an incident must not delay any incident being reported under this procedure.

The person reporting the incident should telephone the Council's Corporate Legal Services incident number **(01926 73 8881)** as soon as possible. They will ask questions required to determine the risk and actions to be taken. Legal Services will report any incidents involving lost or stolen equipment or a network security issue to the ICT Service Desk immediately. For the purposes of this procedure lost or stolen hardware will be logged and may be subject to further investigation depending on the circumstances giving cause to the incident. The Police should be notified immediately of any incidents involving stolen information or equipment and a crime reference number obtained. It is the individuals who has had the equipment stolen that is responsible for notifying the police.

If the information security incident is reported outside of office hours, then a message should be left on the answerphone system.

The incident reporting procedures can be found on the Council's intranet or by via the Information Management data breach and security incident page at: www.warwickshire.gov.uk/imincidents .

6. Incident Classification

The severity of an information security incident will be determined in accordance with the incident levels set out in Appendix A.

An incident will be rated in accordance with the Council's corporate strategy to risk management, which is based on agreed criteria for assessing the likelihood, severity and impact of risk.

Matters to consider would include:

- The nature, sensitivity and volume of personal data;
- Ease of identification of individuals;
- Severity of consequences for individuals;
- Special characteristics of people that may be affected (e.g. age, vulnerabilities);
- The number of affected individuals;

- The nature and role of the Council;
- Nature of breach (e.g. error, mistake or intentional action and malicious);
- Financial or legal implications, and reputational damage.

It is difficult to provide a definitive list of incidents by level as each case varies depending on the circumstances, including containment and recovery, which may reduce or escalate the level at any given point. An initial incident rating will be awarded upon incident notification and may change once the facts and impact of risks has been determined.

Generally the less serious incidents will involve encrypted data or low level data including near misses whereby the severity is reduced due to fortunate events. The more serious incidents will involve high level data which poses actual or potential high risk to people's rights and freedoms or to the organisation e.g. through the loss or release of highly sensitive personal or confidential business information.

7. Notifications

Internal Notifications

Aside from the initial reporting mentioned above internal notifications will be determined in accordance with the incident rating as set out in Appendix A.

It is important to notify key senior staff of the more serious incidents. Human Resources should be notified in the event of disregard for policy or Facilities Management in the event of building security. All incidents involving health and social care data, where there is a risk to any individuals, must be reported to the relevant Caldicott Guardian.

External Notifications

ICO. Any incidents categorised as a high risk may amount to a serious breach and require notification to the Information Commissioner's Office (ICO). In particular, there is a requirement to notify breaches to the ICO where it is likely to result in a risk to people's rights and freedoms. Where information is not available at the time of reporting, it should be provided to the ICO as soon as it is available.

The Incident Lead or Incident Group member who has been allocated the breach to investigate will be responsible for notifying the ICO where appropriate. Monitoring Officer approval will be sought in relation to any incidents requiring notification to the regulator and the Data Protection Officer will be consulted accordingly.

Data Subjects. There is a requirement to communicate a breach to data subjects where there is any incident that it likely to result in a high risk to people's rights and freedoms. The data subject should be provided with:

- the name and contact details of the Incident Lead, Data Protection Officer or another contact point where more information can be obtained;
- the likely consequences of the personal data breach; and

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

NHS Digital. Where public health or adult social care data is involved the incident may amount to a serious incident requiring investigation (SIRI) and require notification using NHS Digital procedures. Depending on the severity this may be notified to the Department of Health (DoH) and Information Commissioner's Office (ICO).

The Incident Lead or Incident Group member will liaise with Information Management to use the IG/Data Protection & Security Toolkit to report this.

The Incident Lead or Incident Group member will provide advice on any other notifications as appropriate for affected stakeholders.

8. Incident Management

An incident flowchart can be found in Appendix B.

Stage 1 – Incident Notification

- Any actual or suspected incident must be immediately reported (and in any event **within 4 hours)** after becoming aware of the incident.
- Telephone the Council's Corporate Legal Services incident number at Shire Hall **(01926 73 8881)** as soon as possible. They will ask questions and record the incident. Any incidents involving lost or stolen equipment or a network security issue will be reported to the ICT Service Desk immediately.
- When reporting the breach, the notifying officer that reports it will be required to provide as many key details of the incident as possible including what happened, when it occurred, what information or assets were compromised, number of people affected and any immediate action taken. Further information can be provided once known by the notifying officer.
- Where a member of the public, information sharing partner or supplier notifies WCC of a breach, they will be directed to the Data Protection Officer in the first instance who will notify Legal Services.

Stage 2 – Incident Assessment

- The severity of an incident will be determined by the incident rating.
- Upon notification an initial assessment of risk will be undertaken by the Incident Lead (or Group Member) to determine a provisional incident rating and appropriate internal notifications will be made as per the applicable rating (e.g. considering likelihood and severity of the risks to the rights and freedoms of data subjects – set out in section 6 above and Appendix A).

- Where incidents are rated as high risk consideration shall be given if a data security breach is to be notified to the ICO or NHS Digital (for public health and adult social care data using the NHS IG Toolkit assessment tool as an initial assessment) (see section 7 above re external notifications). This assessment will be made as soon as possible to ensure that any breach will be reported within a 72 hour deadline (the 72 hours beginning from when the individual is aware of the beach). Any reporting to the ICO or other bodies will involve prior consultation with the Data Protection Officer and will always be subject to Monitoring Officer approval.
- Consideration will also be given as to whether any internal notifications need to be made related to the breach (see section 7 above re internal notifications) and this will be kept under review.
- An incident rating may change once the full facts and impact of risks has been determined and the status of the incident will be kept under review accordingly. In addition, this may involve updating any reports to the ICO and/or other external bodies and internal persons accordingly.

Stage 3 – Incident Investigation

- Not all incidents will require an in depth investigation to establish the facts and determine what went wrong.
- The level of detail provided to ICT/Legal when reporting the breach (together with any information provided in the incident reporting form when completed) should usually be sufficient to understand the incident.
- One of the Incident Group Members will be nominated to review the incident.
- If any additional information is required then the Incident Lead (or Group Member) will contact the notifying officer or any other persons involved in the incident to seek clarification or further information.
- Any incidents rated as medium or high risk may require a full scale investigation in which case the relevant Head of Service will be asked to assign a senior manager to investigate the incident and terms of reference will be agreed by the Incident Lead (or Group Member).
- As mentioned at Stage 2 above, where an incident is high risk and may require reporting to the ICO or any other relevant body, then the relevant Incident Group Member will consult the Data Protection officer and the cyber security/IT team (as appropriate) to further assess the risk and identify and recommendations/actions. This will be done immediately after the high risk incident is reported and a meeting may be convened (remotely or in person) to discuss the matter. Internal notifications should also be considered (see section 7 above re internal notifications).
- The investigation should be completed and returned as soon as possible, taking into account the severity of the incident.

Stage 4 – Incident Review

- The completed incident reporting form and any additional information or investigation report will be reviewed by the Incident Lead (or Group Member).
- A final incident report will be produced within 5-10 days (except in cases of high risk incident, which will be completed sooner where possible) of the investigation being completed setting out (i) observations and conclusions about any information governance non-compliance issues, risks, adverse consequences or implications; and (ii) remedial recommendations to mitigate the risks and impact including preventative measures to address areas for improvement and training needs.
- The completed incident reporting form and any additional information or investigation report will then be reviewed by the Incident Group usually within 5 – 10 working days.
- Any repeat or previous similar incidents will be flagged in the final incident report and may result in additional or escalated action.
- This procedure is independent of a locally commissioned disciplinary investigation but the final incident report may inform any consequential action taken or considered.
- Where a matter has been reported to the ICO or any other statutory body, the relevant Incident Group Member will continue to keep the ICO and other bodies updated accordingly on the investigation, incident review and outcome.

Stage 5 – Incident Resolution

- The final incident report will be sent to the relevant Head of Service to sign off and accept the recommendations by appointing a responsible officer and target dates for implementation.
- It will also be shared with other key staff or specialist units in accordance with the incident rating.
- The signed report should be returned within **5 working days**.
- If for any reason a recommendation is rejected then the Head of Service must specify the reasons why. The Incident Lead (or Group Member) may escalate the matter in order to enforce implementation.

Stage 6 – Incident Monitoring & Closure

- The responsible officer will be required to update a monitoring log for the relevant Service to indicate when recommended action has been implemented by completing the ‘actions taken’ and ‘date action complete’ fields.
- If the incident has been reported to the ICO/NHS or another regulatory body, a final status and update will be recorded.
- HR and Facilities Management will be required to feedback any action taken following disciplinary investigations and facilities or building security checks.
- The Information Governance Lead, Incident Lead (or any other Group member) shall report to the Information Governance Steering Group (IGSG) with any

recommendations for changes to corporate policies, procedures and training including lessons learnt, and shall provide quarterly incident data to Heads of Service and IGSG Representatives.

- An incident will only be closed when all aspects including the monitoring log updates have been completed.

Note:

The Incident Lead (or Group Member) may become involved in an incident at any stage if the investigation is not proceeding to a satisfactory outcome, and the matter may be escalated to Strategic Director/SIRO/Monitoring Officer/Caldicott Guardian/Data Protection Officer if the procedure is not being followed or making adequate progress.

Appendix A - Incident Levels

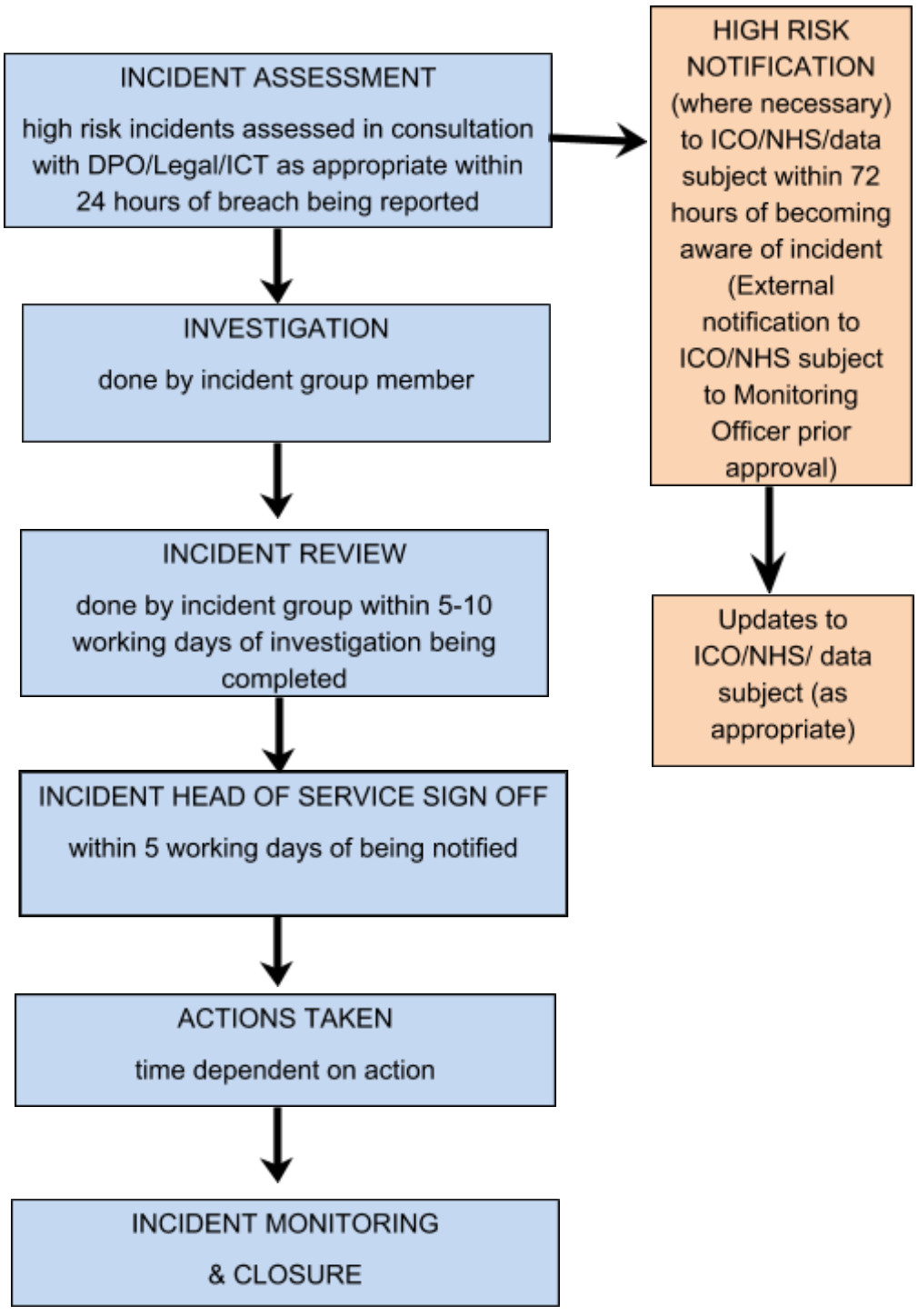
An incident rating will be awarded upon reporting and may change once the full facts or impact of risks has been determined.

Levels	Description	Internal Notifications (as appropriate)
No Risk	No breach as data protected and no impact.	Incident Group (ICT-SD)
Low Risk	Breach of personal or business data but low risk and impact to individuals.	Incident Group, DPO (ICT-SD, HR, FM)
Medium Risk	Breach of sensitive personal or confidential personal or confidential business data and medium risk and impact to individual(s). The personal data breach **is unlikely** to result in a risk to the rights and freedoms of natural persons.	Incident Group, DPO, HoS, CG, SIRO (HR, FM, ICT-SD)
High Risk	Breach of sensitive personal or confidential personal or confidential business data and high risk and impact to individual(s). The personal data breach **is likely** to result in a risk to the rights and freedoms of natural persons. **Decision if to report to data subjects** **Decision if to report to ICO/NHS**	Incident Group, DPO HoS, CG, SIRO, MO, SD, HR (FM, ICT-SD)

Key: ICT-SD: ICT Service Desk, HoS: Head of Service, HR: Human Resources CG: Caldicott Guardian, SD: Strategic Director, SIRO: Senior Information Risk Owner MO: Monitoring Officer, DPO: Data Protection Officer, FM: Facilities Management

Additional points to consider when assessing the incident breach rating:
- The nature, sensitivity and volume of personal data;
- Ease of identification of individuals;
- Severity of consequences for individuals;
- Special characteristics of people that may be affected (e.g. age, vulnerabilities);
- The number of affected individuals;
- The nature and role of the Council;
- Nature of breach (e.g. error, mistake or intentional action and malicious);
- Financial or legal implications, and reputational damage.

Appendix B - Incident Flowchart



Appendix C - Incident Group Terms of Reference

A WCC 'Incident Group' will set out a standard procedure for dealing with information security incidents and the reporting and escalation of such events.

All information security incidents will be dealt with by the Incident Group, which comprises of lawyers from the Council's Corporate Legal Service (Group Members) with a nominated Incident Lead, Information Management and Cyber Security, who will review and advise on incidents and make recommendations on appropriate follow up and corrective action. Cyber Security will implement any immediate infrastructure actions required.

Group Membership

Legal Services, Corporate & Commercial Team: Solicitor (Incident Lead)
Legal Support (Coordinator) Senior Solicitor / Solicitor (Group Member)

Information Management (Group Member)
Cyber Security (Group Member)
Data Protection Officer

Terms of reference

Areas include:

- develop corporate and consistent response to information incidents including any that may be required to be notified to the ICO and communicated to the data subject(s)
- oversee, develop terms of reference for, incident investigations
- offer guidance on data incidents and on best practice
- make recommendations for remedial actions and improvements
- work with the DPO to address and reduce breaches
- link to HR for any possible disciplinary action
- link to Caldicott Guardians for health or adult social care data
- link to Cyber Security or Information Management for any corrective action
- link to Facilities Management for office security and CCTV
- link to Risk and Assurance for corrective action and risk awareness
- report to Senior Information Risk Owner and / or Monitoring Officer
- report to Information Governance Steering Group
- report to regulators as appropriate
- monitor implementation of remedial actions and improvements
- identify trends and areas for greater local or corporate focus.

Appendix D - Cybersecurity Incident Response Procedure

Identification

Potential cybersecurity incidents are investigated by the Information Assets Computer Emergency Response Team (CERT) using information from the following sources:

1. Contact from users: A user or system administrator of a computer system on the WCC network contacts Information Assets and reports indications that their system has been compromised.
2. Contact from external users: Users from remote sites contacts Information Assets CERT with reports that systems under their control have been compromised, and forensic analysis reveals that they had been used to launch attacks against systems on the WCC network.
3. Contact from external organisations: Incident reports/notifications from external security/notification organisations that indicate that a system under our control has been compromised and is launching attacks against systems external to the WCC network.
4. Trouble reports/passive monitoring: Complaints about network performance or routine network analysis reveal excessive or suspicious traffic originating from one or more computers on the WCC network.
5. Active network monitoring: Reports from Intrusion Detection Systems indicates inappropriate, incorrect, or anomalous activity.

Assessment

Once a potential problem has been identified, Information Assets CERT will analyse and attempt to confirm that it is the result of a security incident. This may include traffic flow recording, packet capture and/or contacting the user of the affected system(s).

This allows Information Assets CERT to determine the likelihood that a security incident has occurred and what level of threat it poses to the network as a whole. Occasionally, this process will result in very brief interruptions of network service, but Information Assets CERT will make every effort to minimize these.

Incidents can be broadly categorized as a:

1. Compromised computer is actively causing widespread problems affecting a number of networks or computers either at WCC or elsewhere.
2. Computer is transferring confidential and/or sensitive information to an unauthorized user.
3. Computer, critical to the business functions of WCC, is compromised but is not actively causing problems.
4. Violation is reported to Information Assets CERT via external organisations.
5. Computer is believed to be vulnerable to a known exploit.

Contain and Eradicate

Once a security incident has been positively identified, Information Assets CERT will act to isolate the affected machine(s). Compromised hosts are often the source of DoS attacks,

which greatly degrade the performance of the WCC network, and can also be used as launching points for attacks against other systems, potentially opening the Council to legal liability. Consequently, Information Assets CERT must act to remedy security problems immediately.

In serious cases, Information Assets CERT may be required to work with the Police as directed by the Council.

Notification

In the case of a compromised computer that is actively causing widespread problems affecting networks or computers at WCC or elsewhere, Information Assets CERT will take immediate steps to disconnect the computer from the network, notifying and working with the user.

In the case of a computer which is compromised but not actively causing problems, Network staff will immediately notify the user and request that he/she disconnect it from the network.

In the case of a violation report from an external organisation, Information Assets CERT will disconnect the computer from the network, and request that the user explain their actions and/or allow Information Assets CERT to analyse the system.

Follow up

Once a computer has been disconnected from the network, it is then Information Assets' responsibility to get the disks re-formatted and/or arrange reinstallation of software on the machine and take any other steps necessary to secure it from future attacks. This would depend on factors such as acquaintance with the system in use and whether it had been supplied and configured originally by I.A.

Once the computer is secured, it is the owner's responsibility to contact Information Assets CERT, who will then allow it to be reconnected to the network. At this point, a security scan will be run to verify that the system has been sec0.ured. Results will be forwarded to the computer owner.

Refusal by the system's owner to fully co-operate with requests from Information Assets CERT will be notified to their Head of Service and relevant Strategic Director.

The CERT Team

The CERT Team will be made up from representatives from all relevant areas that need to be involved; this will include (but not limited to):

1. The relevant Business Partner from Information Assets
2. The Technical Security Team
3. Relevant network personnel
4. ICT Communications
5. Senior representative to make strategic decisions efficiently
6. Device Support/ICT Service Desk