Information Security Incident Management

July 2026

Contents

What This Covers

This procedure applies to everyone working for or on behalf of the ST4G/VDS. This includes, but is not limited to, employees, contractors, temporary staff and third parties. It is also applicable to any device, account or system used for our work, whether owned by us or not.

Security Incident Management Procedure

Reporting Information Security Events & Weaknesses

Information security events are reported immediately after they are seen or experienced. This may be verbally or via email to Top Management. Regardless of the initial reporting method, Top Management are responsible for documenting these reports and storing them in a secure location.

Examples of security events are:

- A virus infection on a workstation or server that was not detected and cleaned automatically;
- Loss of equipment;
- Loss of service, functionality, equipment or other facilities;
- System, software or hardware malfunctions, unscheduled shutdowns, unexpected system errors.
- User account credential compromise;
- A user receiving a targeted phishing email.

Examples of security weaknesses are:

- Security risk not being adequately considered for large changes;
- A weak password being used on a service or system;
- Encryption not being set before transferring sensitive information over a public network.

Users should not continue working on the affected asset after identifying a possible weakness or information security event unless instructed by Top Management.

Top Management will work with IT professionals to document how an event or weakness was closed out.

ST4G/VDS operates a ‘no-blame’ culture with regards to reporting information security events resulting from honest mistakes or reports made in good faith. Disciplinary action is still reserved for wilful or reckless misuse.

Assessment of and Decision on Security Events

All information security events and weaknesses are, as soon as possible after receipt, assessed and categorised by Top Management. Initially, there are the following categories:

Category	Description
Events	Occurrences that, after analysis, have no or very minor importance for information security.
Weakness	Vulnerabilities that, after analysis, clearly exist as significant weaknesses compromising information security.

Incidents	Occurrences of events (series of events) that have a significant probability of compromising the organisation's information security.
Breach	Confirmed unauthorised access or egress of information.
Unknown	Those reported events or weaknesses that, after initial analysis, are still not capable of allocation to one of the above four categories.

The 'unknowns' are subject to further analysis to allocate them to one of the other categories as soon as possible.

The prioritisation for responses, when there are multiple event reports to deal with, is as follows: incidents, unknowns, weaknesses, events.

If there are multiple event reports in each category, reports will be prioritised considering the criticality of the business systems and information assets at risk, the danger of further compromise to the organisation's information security and the resources available.

Where necessary, additional input will be sought from qualified technical staff to understand, contain and respond to an incident.

Response to Information Security Incidents

Top Management will invoke actions as necessary to contain and recover from an incident, and to implement a plan of action.

Incidents involving a breach in the confidentiality of personal or client information must be responded to immediately. Clients must be informed without undue delay of a breach identification. Top Management must be involved in all stages of response to breaches of personal or client information. A decision will be made by Top Management as to whether the UK supervisory authority should be notified of a breach as required by UK GDPR. Where this is the case, the ICO will be notified no later than 72 hours after ST4G/VDS became aware of the breach.

Where appropriate, Top Management will coordinate activity with other organisations via email, telephone or any other appropriate means.

Top Management confirms that the affected business systems have been restored and that the required controls are operational before authorising a return to normal working.

Top Management are responsible for closing out an incident, which could include:

- Any reports to external authorities;
- Initiating disciplinary action, if necessary;
- Planning and implementing preventative action to avoid any further recurrence;
- Collecting and securing audit trails and forensic evidence, if required;
- Initiating any required action for compensation from software, service or outsourced suppliers;
- Communicating with those affected by or involved in the incident about returning to normal working.

The response times to reports are determined from the security impact field:

Security Impact Level	Impact Estimation	Priority	Target First Response Time	Target Resolution Time
Negligible	<£1k loss equivalent	Low	5 Days	5 Months
Low	£1-5k loss equivalent	Low	5 Days	3 Months
Medium	£5-10k loss equivalent	Medium	2 Days	1 Months
High	£10-50k loss equivalent	High	2 Days	1 Week
Critical	>£50k loss equivalent	Urgent	1 Day	2 Days

Incident Knowledgebase

Once events, unknowns and incidents have been closed out and a report has been created, they are saved by Top Management.

These reports should include details of:

- The date and time the event occurred, and when Top Management were initially made aware;
- Who initially reported the problem and what happened;
- Whether any personal or client data was involved;
- What was done in response, and who was notified;
- Date closed, and anything that was changed as a result.

If appropriate, a one-off awareness session may be scheduled shortly after an incident has been closed out to educate staff on how to prevent the same thing from happening again.

Collection of Evidence

Where the likelihood of legal, civil or criminal action is established early in the incident response process, the police or lawyers are involved as early as possible, and their guidance is sought and followed in respect of evidence collection and retention.

In these cases, the following guidance must be followed:

- Devices should not be wiped, reinstalled, repaired or ‘cleaned up’.
- All original emails, screenshots and logs should be retained.
- Professional advice should be sought before making any changes to the affected device(s).