DRPG

INFORMATION SECURITY INCIDENT MANAGEMENT

Version:	5
Published:	25/08/2022
Created by:	James Hurley
Approved by:	Richard Parmenter
Confidentiality level:	Restricted

Contents

1 Purpose and scope

The purpose of this policy is to reduce the risk to assets, systems, and data and to ensure data to an affected system can be returned to an operational state as quickly as possible.

All **DRPG** team members, (which include contractors, freelancer's, temporary staff, apprentices and third parties) and all owners of organisational information assets or systems are required to be aware of, and to follow this procedure in the event of an incident.

2 Responsibilities and applicability

Team members are required to report information security incidents, weaknesses, and events to the IT Service Desk, as set out below.

Service Desk Engineers are responsible for monitoring and responding to automated alerts and for reporting those events (or sequences of events) that fall within the scope of this standard.

Where required the Information Security Manager is responsible for coordinating and managing the response to any reported incident, weakness, or event, including documentation of all emergency steps taken, evidence collection, and closing out the event.

All Service Desk Engineers and team members are required to support the Information Security Manager in dealing with an event or weakness.

Where a security incident is suspected or confirmed to have affected personal data, the Data Protection Officer will be informed at the earliest possible opportunity and take responsibility for any DPA 2018 or GDPR compliance requirements.

The CISO or Head of IT authorises access to live systems or data with asset owners carrying out actual access to live systems or data in dealing with an incident.

3 Referenced documents

ISO27001:2013 A.16.1.1 A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7, A.18.2.3
DRPG 130 ISMS 16.1 REC - Incident Report

4 Introduction

The procedures for incident response planning are defined in advance of an incident occurring. The Security Incident Management tracker module in ISMS.online guides an incident through the key states it needs to go through, ensuring that all incidents receive the same structured approach. These are:

- To do
- Assess / Correction or Containment
- Review (and learn) / Root Cause Analysis
- Respond / Corrective Actions
- Resolved
- Archived

The items on the tracker should be used to track all work relating to the investigation and resolution of that incident. If identified as part of that incident that further work is required a project to track that work will be created and linked to that track item.

The CISO in conjunction with the other ISM is responsible for defining the approach to incident management, this includes the other policies within A16 Information Security Incident Management, to ensure that the procedures established provide a clear point of contact for security incident and team members are suitably competent in dealing with those incidents.

Where a security incident is suspected or confirmed to have affected personal data, the Data Protection Officer will be informed at the earliest possible opportunity and take responsibility for any DPA 2018 or GDPR compliance requirements.

Team members are trained on reporting information security events and reporting information security weaknesses as part of Information security awareness, education and training.

For the purposes of the policies in this section we use "security incident" to refer to both "security events" and "security incidents" unless otherwise specified in that control.

5 Reporting Information Security Events

If an information security event occurs or, or is believed to have occurred, it ***must be reported immediately in person, by phone, email or via The Surgery and reported to the Service Desk within 24 hours***. Team Members are made aware of their responsibilities as part of Information security awareness, education, and training.

Possible reasons for reporting a security incident include

- Ineffective security controls.

- Breach of information integrity, confidentiality, or availability expectations.
- Human error.
- Non-compliances with policies or guidelines.
- Breaches of physical security arrangements.
- Uncontrolled system changes.
- Malfunctions of software or hardware or anomalous behaviour; and
- Access violations.

By Phone - If the priority is critical then call the Service Desk on Ext 2060 or 01299 382060. If you need to raise an incident out of hours, then please call the Head of IT by mobile.

By E-mail – support@drpgroup.com to raise an incident electronically but depending on the nature and severity a call would be more preferential. The email address is monitored during working hours and messages sent to it will be flagged for the attention of the ISM.

By completing an Information Security Incident Report via The Surgery or using the *DRPG 130 ISMS 16.1 REC - Incident Report* template on the The Hub.

Upon receipt of any reported incident a unique incident number along with and a priority and severity will be assigned by the Service Desk Engineer in SolarWinds Service Desk where information about the incident can be tracked.

The ISM or an authorised representative will then create an item on the Security Incident Management board within ISMS.online to track, capture, investigate and as appropriate resolve the incident and identified remediations.

In certain circumstances team members may not allowed to continue working on the asset or system after identifying weakness or information security events until given the express consent from the ISM.

6 Reporting Information Security Weaknesses

As with reporting information security incidents (section 5), team members are aware of their obligations to report security weaknesses as part of Information security awareness, education, and training.

On discovering a security weakness, team members must not attempt to prove that weakness as testing it may be interpreted as a potential misuse of the system and may damage information or the system in question

Suspected security weaknesses must be reported as per the instructions in Reporting information security events above.

All Service Desk Engineers are trained to be aware of security incidents (as part of their general first line triage process) and notify the ISM or CISO accordingly in line with the processes described in Reporting information security events.

7 Assessing and Responding to Information Security Events

All reports of information security weaknesses or events relating to any of **DRPG**'s information assets are within the scope of this procedure. In addition, any events or weaknesses detected through the following automated system or application reports will need to be investigated.

- WatchGuard Dimensions
- Sophos Central – Infection/PUA reports
- Manage Engine AD Audit Plus reports
- Nessus Vulnerability Scanning
- Veeam Backup & replication
- NinjaRMM
- Office 365 reports

**Please note this is not an exhaustive list and may not require an incident to be raised.*

When a security event is created on the Security Incident Management Trackere, the first task is to assess the event and then determine a course of action that

- Minimises any compromise of the Availability, Integrity or Confidentially (CIA) of information
- Prevents against further incidents
- Has the minimum disruption to other users of that service
- Considers who needs to be informed; internally, clients, suppliers, regulators e.g. within GDPR and Data Protection Act 2018 requirements.

Security events need to be assessed as follows

- **Security Event** - An action or occurrence that may have (but didn't or hasn't yet) led to information being compromised in terms of its CIA

- **Security Incident** - An action or occurrence that did lead to a compromise in terms of information CIA and can be evidenced to that effect

- **Security Weakness** - A process or flaw in a system that allows a user to compromise the CIA of information held within an information system

Once assessed, a lead for the response to that event is nominated by the ISM and any relevant parties required to support in the resolve of the event are informed.

If the incident affects customer data, the primary contact for that customer/s must be informed immediately and their advice sought as to whether any further notification is required (e.g. ICO/GDPR or GCHQ).

Any requirement for reporting relevant information security events to interested parties and any contact with authorities including customers, suppliers* and regulators** is managed by the Management Review Board, including the CISO as part of its normal operating processes and in accordance with the wider ISMS policies and controls.

The DPO takes responsibility for leading on compliance with the Data Protection Act 2018 and GDPR where personal data is affected.

The item is set to a status of Response on the Security Incident Management track. The details of a response to an Information Security Incident are detailed in Response to information security events.

* Also, in accordance with any specific customer reporting requirements agreed as part of bespoke contracts of major incidents that fall within the GDPR notification for individuals.

**e.g. The Information Commissioner's Office (ICO) as a Supervisory Authority if personal data is affected and is likely to result in a high risk to the rights and freedoms of individuals.

During the assessment, a lead is assigned in the Security Incident Track to respond to the security event. They will be responsible for restoring a normal level of security whilst:

- Collecting evidence as soon as possible after the occurrence.
- Conducting information security forensics analysis, as required in line with Collection of evidence.
- Escalation, as required internally, with specified customers and if appropriate to the relevant information commissioner as part of the GDPR - and tagged accordingly in the Security Incident Track.
- Ensuring that all involved response activities are properly logged in the track item for later analysis.

- Communicating the existence of the information security incident or any relevant details to the CISO, CEO and for them to inform other internal and external people or organisations with a need-to-know; and
- Dealing with information security weaknesses found to cause or contribute to the incident.
- Once the incident is resolved the track item is set to a status of "Review and Learning". In accordance with Learning from information security incidents post-incident analysis should take place, as necessary, to identify the source of the incident.

8 Learning from Information Security Incidents

As part of our commitment to continual improvement we want to ensure that we learn the lessons of any security incident to help evolve and adapt our ISMS.

The use of the Security Incident Management track allows us to review and filter all incidents to help spot trends and areas for improvement. Our process outlined in Assessment of and decision on information security events ensures we are flagging significant events.

Once an incident has been resolved it is set to a status of Review and Learning, and the CISO, ISM and the lead responder for that incident will discuss any changes required to processes of ISMS policies as a result. Any relevant recommendations will then be put to the Management Review Board for ratification or further discussion as required.

In addition, our control to demonstrate how nonconformities and corrective actions will be addressed, will be used where required in particular for repeating issues and where audits expose nonconformance or specific customer complaints arise.

Once the review and learning has been completed and agreed by the core team and updates have been made to ISO policies as required, then relevant team members and any other relevant parties must be notified and trained as appropriate in the new/revised policies and process for that area via our process for Information security awareness, education and training.

9 Collection of Evidence

Where we suspect or know that a security incident may result in legal or disciplinary action, we carry out the following steps:

For digital data on software services, we produce and manage

1 Collect the evidence related to the security incident. This may be exact copies of the entire media or memory. If the incident relates to a remote server, then it may be sufficient to preserve the relevant log files that cover the period of the incident. The collection of evidence will be managed by the ISM and may involve other members of the technical team or the hosting provider if the incident relates to a remote server.

2 Once the evidence has been collected and the ISM is satisfied of its authenticity and integrity it will be signed with the cryptographic key of a person designated by the CISO (in many cases this will be the CISO themselves). This effectively creates a new 'sealed' file that allows recipients of the archive to be sure that the creator of the archive was the designated agent and most importantly that the evidence hasn't been altered since it was archived.

3 The signed file is then uploaded into the relevant place in our environment and also stored in an encrypted form elsewhere for backup. If the marking of the evidence (e.g., for sensitive government data) is considered to be greater than our systems are allowed to hold then we will abide by the prevailing regulations on suitable places where the backup data can be stored.

For digital data on third party systems

1 If the incident took place on a third-party application, we would use the tools provided by that application to gather evidence

2 If required, we will liaise with that provider directly to gather more detail.

3 In these cases, the Information/Asset owner for that system will lead the collection of evidence with the support of the ISM as needed.

4 Evidence collected will be stored securely within our software service as guided by the ISM

For physical media and devices

1 Where an incident has occurred involving physical media or processing devices known to result in legal action (e.g., theft / destruction of data / devices) the relevant authorities must be informed and the collection of evidence, chain of custody etc handled by their specialists.

2 Any physical media relating to the incident must be held securely and without interference by the CEO, CISO or a nominated representative thereof. A note of the chain of custody should be maintained to provide to the relevant authorities.

3 Where an issue may result in disciplinary action the evidence must be taken as soon as practical to the CISO, Head of HR who will ensure its safe keeping whilst disciplinary proceedings progress.

Regulatory and Legislative obligations

All evidence will be retained in accordance with relevant regulations and legislation as outlined in (A.18.1.1) including but not limited to the GDPR, Data Protection Act (2018) and the Police and Criminal Evidence Act (1984).

10 Testing & Monitoring

This Incident Response Standard is reviewed at least annually or upon significant change. Incident reporting is an embedded process of our ISO27001, and the process is subject to internal and external auditing by our chosen external auditing body. All elements of the incident process are evaluated from training, logging, reporting, containment, corrective actions, and analysis to the root cause to ensure that risks have been identified by our 'Risk Assessments' and actions raised to mitigate or accept the risk via Risk Treatment planning.

11 Document owner and validity

The Information Security Manager is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements of the ISMS.
This document is valid from 25/08/2022

Next review date 24/07/2023

12 Change Record

Issue	Description of change	Approved by	Date
1	Initial issue and publication of Work Instruction T – Security Incident Response Standard. This standard was originally three separate policies which have been brought together to form policy.	Richard Reed	25/01/2019
2	Document review and updates outlined below • Added Revision History table • Added correct section numbering • Grammatical and Spelling corrections • Removed references to individual policies ISMS DOC 16.1, 16.2 & 16.3 • Changed Support Technicians to bring into line with current titles of Service Desk Technicians	James Hurley	25/03/2019

	- Corrected and updated incorrect footer - Added section 4. Testing & Monitoring		
3	Document Review and updates	James Hurley	20/01/2020
4	Annual review. - Updated references from Track-it! to SolarWinds. - Updated security reports - Added section 2.12	James Hurley	25/01/2021
5	Annual Review - Updated policy to reflect isms.online trackers - New policy template added	James Hurley	25/08/2022