Incident Management Procedure

PHX032

Contents

Purpose of This Document

The objective of this document is to outline the procedure used for incident management.

Scope

This policy applies to all members of staff and third parties that handle/process secure information including personal data as part of their day-to-day role.

Roles and Responsibilities

Users	Responsibilities
Information Security Committee	• Ensuring the incident is logged • Escalating the incident • Responding to the incident • Communication with interested parties • Handling evidence
Business Continuity Committee	Additional support for ISC in the event of a critical incident impacting continuity of critical business activities.
Environmental Management Committee	Response, investigation and remediation of environmental incidents and events
Infrastructure Team	Response, investigation, and remediation of technical incidents supported by the Security Operations Centre where appropriate.
Senior Management	Management decisions regarding the event
Human Resources	Responding to security incidents in the event of formal disciplinary action
All Staff	All staff have a responsibility for reporting incidents and weaknesses to the business

Types of Events

Phoenix have identified the following types of events that do not lead to an incident:

Event

An event that won't lead to a disruption, loss, emergency, or crisis e.g. a power outage where the generator takes over without fault

Information Security Event

A security event that does not impact the confidentiality, availability or integrity of data or information e.g. blocked scanning attempts within the network permitter

Types of Incidents

Phoenix have identified the following types of incidents:

Incident

An event that could lead to a disruption, loss, emergency, or crisis e.g. a leaking pipe

Information Security Incident

An event impacting the confidentiality, availability or integrity of data or information e.g. System downtime or the unauthorised communication of company information to a third party.

Data Protection Incident

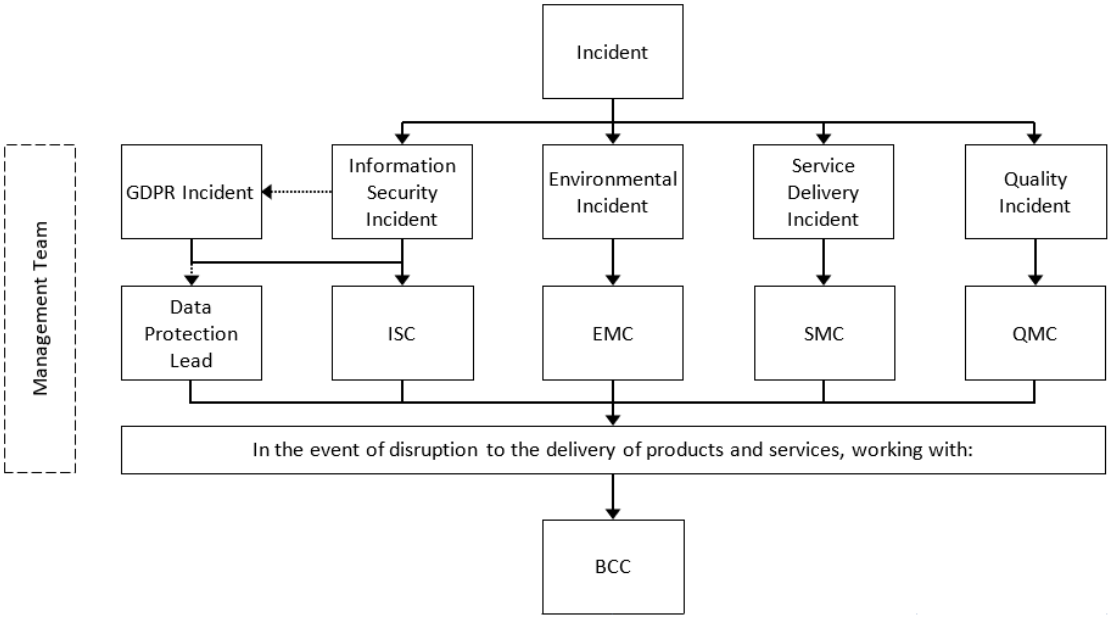
An information security incident with personally identifiable information involved e.g. The communication of an individual's name and address to an unauthorised third party. **See GDPR Manual.**

Disruption

A disruption will be declared if an incident leads to a disruption, loss, emergency, or crisis. A disruption is an incident, whether anticipated or not, causes an unplanned negative deviation from the expected delivery of products and services. The Business Continuity Committee decide whether the business continuity plan will be invoked depending on the circumstances.

A disruption may impact:

- People (staff)
- Information and data
- Physical infrastructure (premises)
- IT systems
- Finance
- Partners and suppliers



Incident Classification

A business continuity incident is a business interruption that prevents Phoenix Software Ltd from delivering its products or services. An incident demands that a process is followed so that the incident is logged, recorded, and resolved. An incident can be an interruption to any process that supports a business service, e.g. failure to access a database or lack of water supply. The aim is that the incident is resolved in such a way that the process can be resumed as soon as possible.

The Incident Manager is the Operations Director. The Deputy Manager is a designated board member.

Incident classification

Impact Category	Category Definition	Business Examples	Factor
Catastrophic	A disaster with a potential to lead to the collapse of the company and is fundamental to the achievement of objectives.	• Major disruption to business continuity resulting in failure to meet SLA and contractual obligations which would trigger an immediate cessation of the contract • Breach of regulatory or legal requirement • Loss of critical/primary business funding source • Business brand damaged • Disruption to entire system or infrastructure which cannot be accommodated by altered operational routines or stand-by infrastructure (i.e., no backup site exists) • Human death suffered.	5
Severe	An event which can be endured but which may have a prolonged negative impact and extensive consequences to the company.	• Serious disruption to business continuity resulting in failure to meet SLA and contractual obligations • Loss of major source of business funding • Disruption to entire system or infrastructure device which can be accommodated by altered operational routines or stand-by infrastructure (i.e., loss of primary processing site where a backup site exists) • Serious or multiple human injuries suffered • Adverse publicity nationally/internationally	4
Material	Major events, which can be managed but that require additional resources and management effort.	• Disruption to business continuity yet still within SLA • Loss of minor source of business funding • Disruption to single critical device which cannot be accommodated by altered operational routines or stand-by component • Significant human injuries suffered • Adverse publicity locally • Some lost time as a result (i.e., less than 1 day).	3
Moderate	Consequences can be absorbed under normal operating conditions.	• Minor disruption to business continuity • Disruption to single critical device which can be accommodated by altered operational routines or stand-by component • Minor human injuries suffered • No lost time as a result.	2
Minor	The impact is minor and can easily be contained.	• Breach of policy but no disruption to business continuity • Disruption to single (non-critical) device which can be accommodated by altered operational routines or stand-by component • No lost time as a result	1

Identify the Incident

IT incidents are identified by using system monitoring tools, cloud-based tools, or scheduled checks. Non-IT incidents are identified by physical methods/indicators.

Log the Incident

The incident is classified and logged on the ISO Measurement Log. The incident log would be maintained within the governance team on SharePoint.

Incident Escalation

For IT or Security incidents the Service Desk Manager or Infrastructure Manager is to be made aware of the business service interruption and any impact known. If the incident is classified as severe, they then must immediately escalate the incident to the Chief Technology Officer or in their absence, the Operations Director followed by the Managing Director. If the incident is designated as a security incident, the Group CISO must also be informed.

For non-IT incidents, the Operations Director, or in their absence the Managing or Finance Director is made aware of the business service interruption and will determine the actions required.

The out of hours escalation is performed via telephone and e-mail. All key staff contact numbers are held by the ISC.

A Director determines if the incident needs escalating to the other directors and communications are drafted for all staff based on severity and scenario.

Incident Resolution

The resolution of an incident will depend on the business area affected and is tested to check the service has been reinstated.

The ISC will communicate with the Board and all employees when the incident has been resolved.

Reporting

Reporting to the business

All employees have a responsibility for ensuring that incidents and potential weaknesses are reported to the business as quickly as possible.

Examples of incidents:

- loss or theft of information
- loss or theft of personal information
- loss or theft of computer equipment, mobile phones, or media
- unauthorised transfer or disposal of Internal Use or Confidential Information
- ineffective security control
- breach of information integrity, confidentiality, or availability expectations
- human errors
- non-compliances with policies or guidelines
- breaches of physical security arrangements
- uncontrolled system changes
- malfunctions of software or hardware
- unauthorised access
- fraud
- any observed or suspected information security weaknesses in systems or services

Malfunctions or other irregular system behaviour may be an indicator of a security attack or actual security breach and should therefore always be reported as an information security event. Employees and contractors should not attempt to try and prove a security weakness.

Testing may be interpreted as a potential misuse of the system and could also cause damage to the information system, service, or compromise evidence, which could result in legal liability for the individual.

Reporting to interested parties

A data protection incident must be reported to the Information Commissioners Office (ICO) in the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

These incidents are to be owned by the Governance Manager who is responsible for reporting to the relevant parties.

If the Personal Identifying Information breach poses a high risk to the individuals effected, they must also be informed of the incident.
It may also be appropriate to report to, and liaise with, law enforcement agencies such as Action Fraud.

Any security event or incident must be reported to the Infrastructure Manager.
Any incidents that are classified as Material, Severe or Catastrophic must also be reported to the Group CISO. See escalations.

Logging the Event

The Information Security Committee is responsible for documenting incidents on the log. The information documented ensures incidents have appropriate corrective and preventative actions and also informs root cause analysis and lessons learnt where appropriate.

Classifications

For information on classifying severity levels for security events, please refer to the **Incident Classification** table earlier in this policy.

Escalations

Where applicable the business may escalate the issue.

Escalations can be done both in house or externally, escalations externally must be authorised by a member of the Senior Management.

Examples of who may be involved in an escalation:

- Senior Management
- Human Resources
- Asset Owner
- Information Commissioner's Office
- Legal Authorities
- Government Authorities
- Customers
- Suppliers

The escalation of information security incidents to the Bytes Technology Group CISO is decided by the Information Security Committee depending on the circumstances and the severity of the events.

The Incident Manager is responsible for ensuring the below escalations take place at an appropriate time:

Incident classification	**Escalation point**
Minor	-
Moderate	-
Material	Senior Management – Executive Committee
Severe	Phoenix Board
Catastrophic	BTG Group level - Neil Murphy, Andrew Holden, Steve Marshall

Investigation

All incidents will be investigated to determine the facts and any corrective actions that are needed. The amount of investigation needed is dependent on the event.

The focus of the investigation is to restore business-as-usual, follow GDPR legislation and for continual improvement within processes and systems.

The appropriate Committee investigates the incident to determine:

- the extent of the event
- the amount and classification of information involved
- the potential for loss or damage
- what actions need to be taken and how quickly to address:
    - restoring any lost information
    - restoring business activities
    - whether to warn people about the loss, including who and when
    - whether to report the incident to:
        - Group level
        - the Information Commissioner Office within a 72-hour window if it involves personal data in line with GDPR legislation
        - the Police

The investigation process may include:

- interviews, formal or informal, with the parties involved
- meetings as appropriate, involving people who can assist in remedying the incident
- involving the Senior Management team to advise on:
    - reporting to the Information Commissioners Office
    - informing interested parties
- consider measures that can be put in place to eliminate or reduce the chances of a re-occurrence
- involve legal services where there is a risk of a claim against the organisation and update log

Invoking the Business Continuity Plan

The invocation of the full recovery of all business services due to a catastrophe is decided upon by the board of directors in discussion with the business continuity management team.

See the Business Continuity plan.

Collection of Evidence

When an event is first detected, it may not be obvious whether or not the event will result in court action. The danger, therefore, exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realised. It is advisable to seek ICO guidance, legal advice or contact the police early in any contemplated legal action and take advice on the evidence required.

The Information Security Committee is responsible for ensuring the accurate collection of evidence, this may involve seeking external resources and should take into account:

- chain of events
- safety of evidence
- safety of personnel
- roles and responsibilities of personnel involved
- competency of personnel
- documentation
- briefing

Closure and Follow-ups

Major incidents will be treated with the utmost urgency until closure and corrective action is in place.

All incidents logged will be reviewed as part of a Management Review and the appropriate Committee will identify trends when available, potential improvements to processes, lessons learnt and additional training requirements.

Any risks identified as a result of the incident occurring will be logged and corrective actions identified.

A follow-up meeting takes place on any actions to ensure they have been completed. The incident is closed once all actions are complete.

Version Control

Author	Version	Date	Description
ISC	1.0	01/07/2015	Original
ISC	2.0	29/01/2018	Include GDPR legislation
ISC	3.0	01/04/2020	Annual Review
ISC	4.0	05/05/2021	Annual Review / No Changes
Amy Trimble	5.0	17/03/2022	Update to reflect ISO22301 and ISO27001:2022 requirements.
ISC	6.0	02/08/2022	Align risk descriptors with Risk Register

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	01/07/2015	Managing Director
Sam Mudd	2.0	29/01/2018	Managing Director
Sam Mudd	3.0	01/04/2020	Managing Director
Sam Mudd	4.0	05/05/2021	Managing Director
Clare Metcalfe	5.0	12/01/2022	Operations Director
Clare Metcalfe	6.0	30/09/2022	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 30/09/2022