Document ID	POL002
Document Title	InfoSec and Cyber Incident Management Policy
Author	Kevin Beadon & Steve Marshall
Version	2024.06.1
Classification	Controlled

Revision History		
Date	**Version**	**Change**
20/06/2022	1.30	Annual review
28/06/2023	1.40	Annual review
21/05/2024	2024.05.1	Alignment of policy with new Incident Management Plan
17/06/2024	2024.06.1	Signoff

Distribution		
Date	**Version**	**Distribution**
08/06/2020	1.10	All staff via Intranet and Library
30/06/2021	1.20	All staff via Intranet and Library
30/06/2022	1.30	All staff via Intranet and Library
28/09/2023	1.40	All staff via Intranet and Library
18/06/2024	2024.06.1	All staff via Intranet and Library

Signed			
Date	**Version**	**Name**	**Role**
08/06/2020	1.10	Keith Richardson	CFO
30/06/2021	1.20	Dave Rawle	CTO
30/06/2022	1.30	Dave Rawle	CTO
28/06/2023	1.40	Sam Kynaston	Digital Transformation Director
17/06/2024	2024.06.1	David Rawle	CTO

Contents

Introduction

The specific purpose of this policy is to ensure consistent management of information security (InfoSec) and cyber incidents, to minimise any harm to individuals or organisations. This policy is not intended to consider the impact and protection of the company's assets from accidents, such as fire, flood, failed hardware, or software.

Intended Audience

This policy applies to all:

- Employees of Bytes Software Services, including senior and executive management.
- Contractors, temporary staff, consultants, or others employed by Bytes Software Services.
- Any other users of Bytes Software Services' IT facilities.

What is a Security Incident?

A security incident can range from a serious data security loss to a relatively minor breach of security procedures. Incidents may be the result of malicious intent, or they may be caused by human error, accident, or force majeure. Likewise, the impact of a security incident may be minor, or it can have a major impact on the organisation. This impact may be experienced in several ways, and these can include:

- The availability of data or related services.
- The authenticity of data or related services.
- The integrity of data or related services.
- The confidentiality of data or related services.

Examples of information security incidents can include, but are not limited to, the following:

- Disclosure of confidential information to unauthorised individuals.
- Loss or theft of paper records, data or equipment, such as tablets, laptops and smartphones, on which data is stored.
- Inappropriate access controls allowing unauthorised use of information.
- Suspected breach of Bytes' IT policy.
- Attempts to gain unauthorised access to computer systems, e.g. hacking.
- Records altered or deleted without authorisation by the data "owner".
- Virus or other security attack on IT equipment, systems or networks.
- Breaches of physical security e.g. forcing of doors or windows into secure room, or opening filing cabinets containing confidential information left unlocked in an accessible area.
- Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information.
- Covert or unauthorised recording of meetings and presentations.

In turn, these security incidents can have further consequences, for example:

- Damage to reputation.
- Decrease in customer or supplier confidence.
- Financial losses.
- Legal liabilities under criminal or civil law.

If you are in any doubt about whether a security incident has occurred, then it should be reported so that it can be investigated, and a decision made. Do not assume that someone else will report this so that you do not have to; failure to report incidents usually means that no one knows about them.

Reporting an Incident

All actual or suspected physical, InfoSec and cyber security incidents must be reported immediately to the IT team using one of the contact methods below:

- E-mail: helpme@bytes.co.uk
- Phone: +44 (0)1372 418504
- Web: https://helpme.bytes.co.uk
- Visit the Systems Support team in Leatherhead.

The IT team or SOC Analyst must:

- Create a helpdesk or SOC ticket with the relevant information.
- Identify the scope and type of incident, including its classification as INFORMATIONAL, MINOR, MAJOR, or CRITICAL (see "Incident Severity" below).
- Notify the appropriate personnel based on the severity of the incident.

If the incident occurs out of hours the on-call person assumes the responsibilities to investigate until they can get hold of a more senior member of staff. Where possible, it is the on-call persons responsibility to decide on the course of action. This person will be supported in the decisions that they make, and their default course of action should be to fail the company safe. If there are any unknowns or the course of action is unclear, fail the company safe, and when more senior personnel are available, they can rectify any actions that are taken.

Incident Severity

Incidents will normally be classified by the first responder that picks them up, and this will either be the Helpdesk (IT) or the Security Operations Centre (SOC), based on the perceived impact to the company's resources and the type of data which could have been impacted:

Incident Severity	Confidentiality Impact	Integrity Impact	Availability Impact	Incident Type	Example
CRITICAL (P1)	Potential, undefined loss of data, outside of the business; or Complete loss of data, outside of business.	Significant system modification and loss of integrity; or Complete loss of control.	Significant or partial loss of availability of system or service, or Complete loss of services, outage, denial of service.	Any incident that, if made public, would affect the confidence of customers and/or shareholders.	Data security breach, attack on the websites which brings it down for an extended period, leak of confidential documents (emails etc), a PCI DSS or Data Privacy incident.
MAJOR (P2)	Is likely to lead to data loss if unmitigated.	Is likely to lead to result in system modification if unmitigated.	Is likely to lead to / cause service availability issues, if unmitigated.	Specific security incidents whose effect is mainly internal and does not affect customers or shareholders.	Unauthorised access of information systems containing sensitive information.
MINOR (P3)	Has potential to lead to data loss if unmitigated.	Has potential to lead to system modification.	Has potential to cause service availability issues, if unmitigated.	Security threats and issues that are discovered and require resolution before escalation of severity can occur.	Compliance issues, new security threats.
INFORMATIONAL (P4)	No impact; or May contribute to data loss if further vulnerabilities are exploited.	No impact; or May contribute to system modifications if further vulnerabilities are exploited.	No impact; or May contribute to system availability if further vulnerabilities are exploited.	Security threats that may affect the business at some point in the future (i.e. end of life notification, attacker activity in industry sector).	Things that may in the future affect the confidentiality, integrity, or availability of data / systems / services.

Roles and Responsibilities

Roles

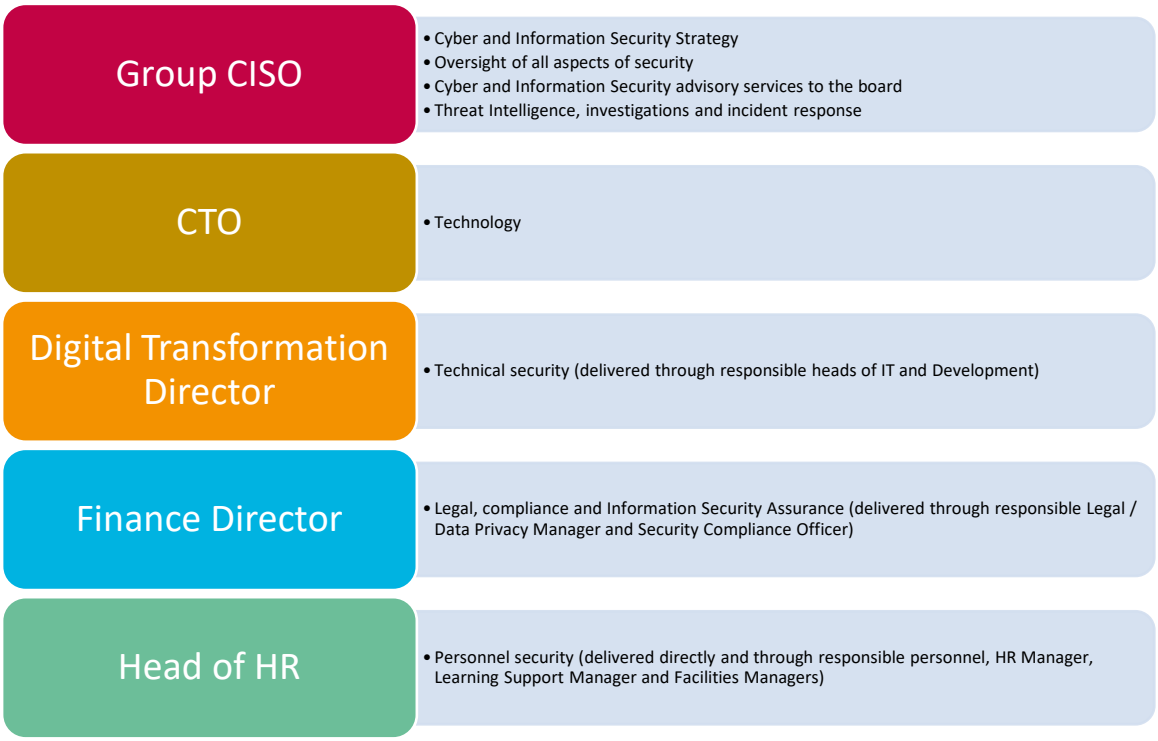
The table below shows the groups or individuals, the associated roles within the organisation involved in the incident management processes:

Group / Individual	Roles
SOC	Initially detect and investigate security events, offences, incidents, and breaches within the organisation.
SOC-TI	The SOC-TI team are responsible for ensuring that the TI data is monitored and fed to the SOC team.

Group / Individual	Roles
Bytes SOC Analyst	Review SOC information by following the "InfoSec and Cyber Incident Management Plan" to confirm SOC information and escalate as required.
Helpdesk	Manage user interactions and reports as well as basic IT functions.
Infrastructure	Responsible for all servers, networking, and technical security equipment, as well as ensuring that all logs are delivered to the SOC team.
Digital Forensics	When called in by the Incident Management Team (IMT) or IT, they will investigate findings.
Penetration Testing	When called in, they test the infrastructure for vulnerabilities and exposure.
Head of IT	Delivery of IT services and a member of the IMT.
Digital Transformation Director	Delivery of transformation projects, responsible for IT and Development teams.
CISO	Cyber strategy, oversight, TI, Incident processes and investigations. Primary Incident Commander of the IMT for P1 incidents.
CTO	ExCo Director and to select technology in use. Key member of the EMT and Secondary Incident Commander of the IMT for P1 incidents, but not if representing EMT.
ExCo	Make decisions and commit the company based on information received from the IMT. Constituent members of the EMT.
Group Board	To handle any comms for impact to the wider group or shareholders.
Service Owner	To provide specific information in relation to the service, customers, data, setup and/or third parties.
Department Affected	To provide specific information in relation to the service, customers, data, setup and/or third parties.
Rest of the Business	To report incidents and follow policies and instructions.
Law Enforcement	To provide law enforcement input into processes and investigative capacity if required.
Competent Supervisory Authority	To provide regulatory requirements or specialist input.

Responsibilities

The Managing Director (MD) is accountable for information security within the organisation, but information security shall be understood, implemented, and maintained by Bytes employees through its procedures and control documentation daily. The following positions have been nominated by the MD as responsible for specific aspects of security under the ISMS, including for incident response:



RASCI matrix

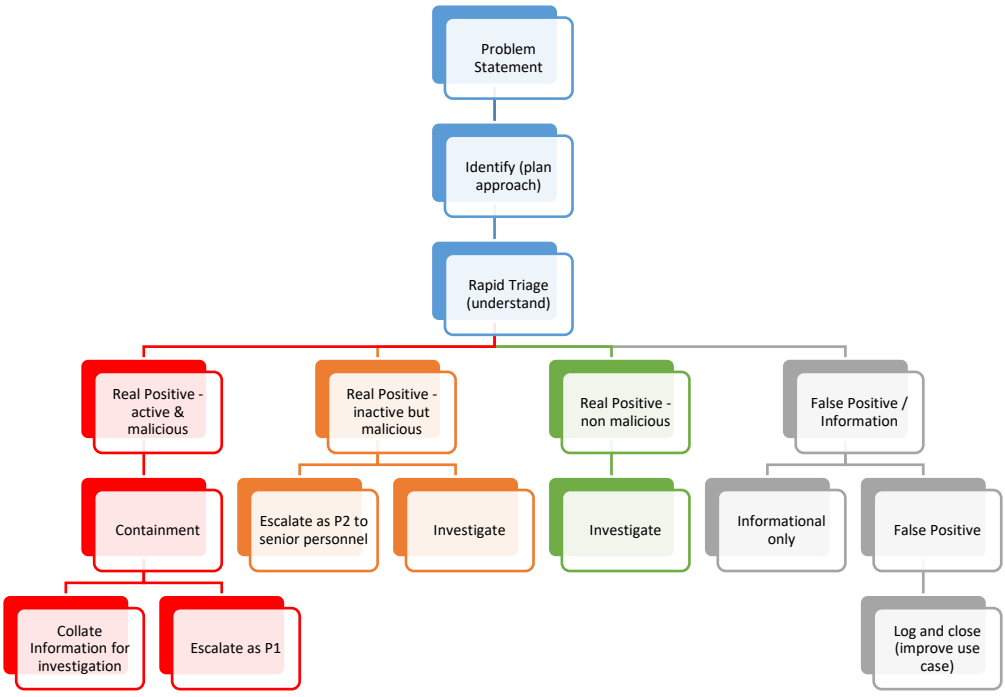
The following RASCI matrix will be used for incident management within Bytes:

Group / Individual	Responsible	Accountable	Supportive	Consulted	Informed
SOC			X		
SOC-TI			X		
Bytes SOC Analyst			X		
Helpdesk			X		
Infrastructure			X		
Digital Forensics			X	X	
Penetration Testing			X		
Head of IT	X				
Digital Transformation Director	X				
CISO	X				
CTO	X				
ExCo		X			
Group Board					X(1)
Service Owner	X				
Department Affected				X	
Customers					X(1)
Rest of the Business					X(1)
Law Enforcement				X	X
Competent Supervisory Authority				X	X

Note: (1) = Informed as required or affected.

Security Incident Management - Initial (all incident severities)

Once the ticket has been created, the SOC Analyst, Infrastructure Engineer or on-call representative should use the following process to manage the incident:



This is a slightly modified process from the general incident management process. This has been taken into an operational process designed for speed, the reason for this is that at the initial point you do not know if the incident is real or a false positive. The idea is to use techniques to analyse this quickly, make a decision, and then conduct the required activity. The InfoSec and Cyber Incident Management Plan should be used from this point forwards to handle the investigation.

Review of Policy

Head of IT, Group CISO, CTO and Data Protection Manager are responsible for reviewing the InfoSec and Cyber Incident Management Policy annually, or after a P1 incident.