Document ID	POL002
Document Title	Information Security Incident Management Policy
Author	Kevin Beadon
Version	1.40

Revision History		
Date	Version	Change
28/09/2017	1.00	New Document
08/06/2020	1.10	Annual review
30/06/2021	1.20	Annual review
20/06/2022	1.30	Annual review
28/06/2023	1.40	Annual review

Distribution		
Date	Version	Distribution
28/09/2017	1.00	Sara Mitchell (DPC)
28/09/2017	1.00	All staff via Intranet and Library
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

Signed			
Date	Version	Name	Role
28/09/2017	1.00	N/A	N/A
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

Next Review: 30/06/2024

Contents

Introduction

The specific purpose of this policy is to ensure consistent management of information security 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.

This policy provides the necessary information for the management and reporting of:

- Security incidents affecting Bytes Software Services and IT systems
- Loss of information
- Near misses and information security concerns

Intended Audience

This policy applies to all:

- Employees of Bytes Software Services, including senior and executive management
- Contractors that make use of Bytes Software Services IT facilities
- IS Manager, IT Manager or Manager responsible for any element of Bytes' IT Systems

Policy Details

Overview

An information security incident is any event that has the potential to affect the confidentiality, integrity or availability of Bytes information in any format.

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 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

Lines of Responsibility

All users who are given access to Bytes information, IT and communications facilities are responsible for reporting any actual or potential breach of information security promptly in line with Reporting an Incident.

All users are responsible for identifying risk to information security and ensuring that it is reported accordingly. The user reporting the incident or appropriate person may then be asked to assist with investigating and mitigating the risk. Any breach should be reported to the Head of IT (or equivalent) immediately

Head of IT (or equivalent) is responsible for leading the activity required to respond to an incident. Activities include reporting to the Financial and Operations Director and the Data Protection Co-ordinator, investigating and taking appropriate action to address breaches of IT systems and network security, and for escalating incidents to the Financial and Operations Director (or equivalent) and the Data Protection Co-ordinator

Chief Technology Officer (or equivalent) has Board level responsibility for reporting any serious information security breach to EXCO and ensuring that appropriate actions are taken to address the breach.

Data Protection Co-ordinator is responsible for ensuring that new systems meet the requirements of GDPR and therefore have had information security considered during deployment and on-going management. Has responsibility for ensuring that reporting to relevant people in the business, and appropriate actions are taken to address breaches. May be required to report breaches to third parties.

Account Managers are responsible for reporting any breaches to affected customers or third parties

Review of Policy

Head of IT (or equivalent), Chief Technology Officer (or equivalent) and Data Protection Co-ordinator are responsible for reviewing the Information Security Incident Management Policy annually or after a serious and significant breach.

Reporting an Incident

An incident should be reported using any of the following methods:

- E-mail helpme@bytes.co.uk
- Call 01372 418504
- Web https://helpme.bytes.co.uk
- Visit the Systems Support team in Leatherhead

When an incident is reported it will be entered into the Company's call logging system, and the Head of IT will be informed. The breach will be categorised as follows:

Serious breach includes, but not limited to, loss or potential loss of personal data about a Bytes employee, customer or supplier and/or the transfer of personal data to unauthorised third parties

Significant breach includes, but not limited to, loss or potential loss of non-personal customer data that Bytes host

Other breach includes, but not limited to, loss or potential loss of non-personal data

If the breach is categorised as 'serious' or 'significant' the Finance & Operations Director will be informed. All information security breaches are reported to the Data Protection Co-ordinator. If necessary, the Data Protection Co-ordinator will report the breach to the relevant Bytes Account Manager who will then inform their affected customer

Representatives of the Head of IT looking into security breaches will be responsible for updating, amending and modifying the status of incidents in the Company's Service Desk system.

Acting on an Incident

All parties dealing with security incidents shall undertake to:

- Analyse and establish the cause of the incident and take any necessary steps to prevent recurrence;
- Report to all affected parties and maintain communication and confidentiality throughout investigation of the incident;
- Identify problems caused as a result of the incident and to prevent or reduce further impact;
- Contact 3rd parties to resolve errors/faults in software and to liaise with the relevant departmental personnel to ensure contractual agreements and legal requirements are maintained and to minimise potential disruption to other Bytes systems and services;
- Ensure all system logs and records are securely maintained and available to authorised personnel when required;
- Ensure only authorised personnel have access to systems and data;
- Ensure all documentation and notes are accurately maintained and recorded in the Company's Service Desk system and are made available to relevant authorised personnel;
- Ensure all authorised corrective and preventative measures are implemented and monitored for effectiveness;
- The Data Protection Co-ordinator will maintain a log of all security breaches;

- Serious incidents will be presented to the Bytes Software Service Board;
- Serious breaches will need to be reported to the Information Commissioner by the Data Protection Co-ordinator;
- All incidents logged within the Company's Service Desk system shall have all details of the incident recorded including any action/resolution, links or connections to other known incidents. Incidents which were initially resolved but have recurred will be reopened or a new call referencing the previous one will be created;
- Monthly reports on incidents generated by the Service Desk system are automatically sent to the Head of IT to facilitate the monitoring of the types, numbers, frequency and severity of incidents which will help to correct and prevent incidents recurring;
- During the incident investigations, hardware, logs and records may be analysed by Bytes' internal Audit function. Information and data may be gathered as evidence to support possible disciplinary or legal action. It is essential that confidentiality is maintained at all times during these investigations.