Document ID	POL010
Document Title	Information Security Policy
Author	Kevin Beadon
Version	1.91

Revision History		
Date	Version	Change
05/02/2018	1.00	New Document
05/02/2018	1.10	Update after Paul Wheaton Feedback
07/02/2018	1.20	Update after Sara Mitchell Feedback
04/09/2019	1.30	Update to reflect ISO270001 requirements
04/12/2019	1.40	Updated to reflect POL019 – Network Systems Monitoring Policy
08/06/2020	1.50	Annual review
09/02/2021	1.60	Updates to reflect observations from ISO27001 review
27/10/2021	1.70	Update to reflect password policy change
30/06/2022	1.80	Annual review
28/06/2023	1.90	Annual review
29/04/2024	1.91	Minor changes ref number for BCM Policy and Strategy now updated

Distribution		
Date	Version	Distribution
05/02/2018	1.00	Paul Wheaton, Sara Mitchell
05/02/2018	1.10	Paul Wheaton, Sara Mitchell
07/02/2018	1.20	Paul Wheaton, Sara Mitchell, Keith Richardson
12/02/2018	1.20	All Staff via Intranet and Library Drive
04/09/2019	1.30	Keith Richardson, Sara Mitchell
18/09/2019	1.30	All Staff via Intranet and Library Drive
04/12/2019	1.40	Keith Richardson, Sara Mitchell
19/12/2019	1.40	All Staff via Intranet and Library Drive
08/06/2020	1.50	All Staff via Intranet and Library Drive
09/02/2021	1.60	David Rawle, Keith Richardson, Steve Marshall, Sara Mitchell
27/10/2021	1.70	All Staff via intranet and Library Drive
20/06/2022	1.80	All Staff via intranet and Library Drive

28/06/2023	1.90	All Staff via intranet and Library Drive	
Signed			
Date	Version	Name	Role
05/02/2018	1.00	N/A	N/A
08/06/2020	1.50	Keith Richardson	CFO
09/02/2021	1.60	Keith Richardson	CFO
27/10/2021	1.70	David Rawle	CTO
30/06/2022	1.80	David Rawle	CTO
28/06/2023	1.90	Sam Kynaston	Digital Transformation Director

Next Review: 08/06/2024

Contents

Introduction

The purpose of this policy is to:

- Define the information security standards of Bytes Software Services (Bytes/Company).
- Establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Bytes Software Services.
- Protect from all threats, whether internal or external, deliberate or accidental the information assets of:
    - Bytes
    - Customers
    - Suppliers

Objectives and Goals

The implementation of this policy is important to maintain and demonstrate our integrity in our dealing with customers and suppliers.

It is the policy of Bytes to ensure:

- Information is protected against unauthorised access
- Confidentiality of information is maintained
- Information is not disclosed to unauthorised persons through deliberate or careless action
- Integrity of information through protection from unauthorised modification
- Availability of information to authorised users when needed
- Regulatory and legislative requirements will be met
- Business continuity plans are produced, maintained and tested as far as practicable
- Information security training is given to all employees
- All breaches of information security and suspected weaknesses are reported and investigated

It is the objectives of Bytes to:

- To continually strengthen and improve the overall capabilities of the information security management system.
- To increase professional skills in terms of information security management and technology.
- To make Bytes' management system for information security so complete and reliable that the ISO/IEC 27001 certification standard will continue to be effective.
- To ensure that information-related business operations continue to be carried out in line with the ISO/IEC 27001 standard and to establish a sustainable operation plan for the business that is cost-effective.
- To establish quantified information security goals annually through management and review meetings.

Supporting Policies

The following documents support this policy:

- POL001 - Firewall Policy
- POL002 – Information Security Incident Management Policy
- POL003 – Incident and Problem Management Policy
- POL005 – Software Patching – Internal Systems Policy
- POL006 – Software Patching – Snow Systems Policy
- POL008 – Malware Incident Management Policy
- POL009 – Backup Policy
- POL011 – IT User Policy
- POL012 – Remote Access Policy
- POL013 – Change Management Policy
- POL014 – User Management Policy
- POL015 – Servers Access Policy
- POL016 – Cryptographic Controls Policy
- POL038 – Business and Continuity Management Strategy and Policy
- POL017 – Remote Access and Teleworking Policy
- POL018 – Access Policy
- POL019 – Network Systems Monitoring Policy
- POL020 - ISO 27001 risk assessment and acceptance criteria (Policy & Procedure)

Scope

This policy, and supporting procedures, encompasses all system resources and supporting assets that are owned, operated, maintained, and controlled by Bytes. It covers the following areas:

- Users access and controls.
- Resource access logs and violation reporting.
- General classification of data.
- Basic data protection requirements.
- Storage media.
- Data transfer.
- Information awareness training.
- Responsibilities for information Security.
- Physical security of IT equipment.
- Terminated employees.
- Accessing customer data

Policy Details

Overview

This policy sets out the policies for information security and how it is applied to Bytes.

Lines of Responsibility

All users – Are responsible for:

- Complying with information security policy and procedure.
- The operation security of the information systems they use.
- Complying with the security requirements that are currently in force.
- Ensuring the confidentiality, integrity and availability of the information they use and that it is maintained to the highest standard.

Information owners (Managers) are responsible for:

- Helping with the security requirements for their specific area.
- Determining the privileges and access rights to the resources within their areas.

Systems Support Team is responsible to the Head of IT and they:

- Ensure the implementation and operation of IT security.
- Ensure the implementation of the privileges and access rights to the resources.
- Support information security policies.

Head of IT (or equivalent) is responsible for:

- The security of IT infrastructure.
- Planning against security threats, vulnerabilities and risks.
- Implementing and maintaining the information security policy document(s).
- Ensuring IT infrastructure supports the information security policy.
- Responding to information security incidents.
- Systems Disaster Recovery plans.
- Validating security training plans.

Finance and Operations Director (or equivalent) has Board level responsibility for Information Security within Bytes Software Services.

Review of Policy

Head of IT (or equivalent) and Financial and Operations Director (or equivalent) are responsible for reviewing the Information Security Policy annually or after a serious issue.

User Access and Controls

- Any system that handles valuable information must be protected with a password-based access control system.
- Every user must have a separate, private identity for accessing IT network services.

- Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
- Discretionary access control list must be in place to control the access to resources for different groups of users.
- Cloud services must support SAML2 and authenticate to the Bytes Office 365 tenant
    - At least 2FA must be used to access all cloud services
    - Where a cloud service does not support SAML 2
        - It must support 2FA
        - Bytes Board must agree to its usage
- Mandatory access controls should be in place to regulate access by processes operating on behalf of users.
- Access to resources should be granted on a per-group basis rather than on a per-user basis.
- Access shall be granted under the principle of "least privilege", i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform their business functions.
- Whenever possible, access should be granted to centrally defined and centrally managed identities.
- Users should refrain from trying to tamper or evade the access control to gain greater access than they are assigned.
- Automatic controls, scan technologies and periodic revision procedures must be in place to detect any attempt made to circumvent controls.
- Using administrative credentials for non-administrative work is not allowed.
- IT administrators must have two set of credentials: one for administrative work and the other for everyday work.
- Test accounts are allowed but cannot be used for Administrative or everyday work and should be deleted as soon as they are no longer required.

Password

Passwords must meet the following complexity requirements:

- Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least 14 characters long.
- Administrative passwords must be at least 10 characters long.
- Each regular user may use the same password for no more than 40 days and no less than 3 days.
- A password history of at least 10 passwords must be kept.
- Password for some special identities will not expire. In those cases, password must be at least 14 characters long.
- Whenever a password is deemed compromised, it must be changed immediately.
- Sharing of passwords is forbidden. They should not be revealed or exposed to public sight.
- Identities must be locked if password guessing is suspected on the account.

Resource access logs and violation reporting

- Systems should report successful and unsuccessful log on attempts.
- Systems Support will maintain a process for searching audit logs.

General Classification of Data

All data within Bytes Software Services is regarded as business confidential unless otherwise stated.

Business confidential data:

- Should not be shared with people outside of the organisation without prior approval by EXCO.
- Should only be shared within the business on a least privilege model.
- Should only be stored on Bytes controlled systems.
- Should be secured by an individual user ID and Password.

Special category data:

- Is only stored by HR and located within the HR System or on the HR area of the file server.
- Access is given on a least privilege model and authorised by HR or EXCO only.

See Data Classification document GDPR_Data_Classification.pdf (bytes.co.uk) for details.

Basic Data Protection Requirements

All Bytes Software Services controlled systems containing personal information as defined in the Data Classification document must be protected in alignment with corporate standards and best practice.

Specifically, where a system is in the:

- Production and DR datacentre.
- Bytes Software Services office corporate network.

A system must operate:

- Up to date anti-malware.
- Be appropriately patched.

Where a system (including laptops and mobile phones) is operated outside of these environments the device must also operate:

- Encryption.

Storage media

Backups must be encrypted in line with industry best practice and hosted in a physical secure environment to protect against loss. Backup media must be stored in one of the following locations:

- Leatherhead datacentre.
- DR datacentre.
- Inside a locked fire safe located within a Bytes Software Service office.

Only Systems Support approved USB memory drives/stick or similar type devices are to be used on Bytes servers. Approved devices will be stored in the Removal Media Log.

Media that is used to store Bytes data must be returned to the Systems Support for destruction, this includes but limited to servers' hard disks, USB drives, laptops and desktops.

Any media that will be reused outside of Bytes must have their media wiped to UK Government standards.

Data transfer

Data transfer containing personal, business confidential or special category data must follow either of the following rules:

- When transferred outside of the organisation on a network it must be via secure mechanisms such as TLS or the data must be encrypted.
- When transferred on a portable device such as a flash drive or laptop outside of the organisation it must be encrypted.

Information awareness training

- Information security training must be given to all staff during their induction.
- Ongoing training must be given at regular intervals to ensure that all staff are aware of current policies.

Physical Security of IT Systems

IT Systems that store data or provide access to data must be in a server room:

- That is locked and controlled separately by key card.
- That has environmental monitoring and alerting.
- Where access to the server room is logged and a reason recorded.
- Where access is by authorised personnel only.
- That is in an area not open to the general public.
- Within a building that has CCTV.
- That has UPS.
- That has a generator.
- That has air conditioning.

IT Systems that are in remote offices can only be used for authentication, routing of network or storing non-personal data other than personal data that is required for authentications purposes. These IT Systems must be in a server room:

- That is locked.
- That has environmental monitoring and alerting.
- Where access is by authorised personnel only.
- That is in an area not open to the general public.

Terminated Users

A terminated user includes all users that are no longer employed or contracted by Bytes Software Services. On a user's last day, the following must be executed or configured:

- The terminated users account(s) must have the password changed.
- All access to IT Systems will be revoked.
- All Bytes Software Services IT supplied equipment must be returned.
- If for any reason the user is keeping Bytes supplied IT equipment it must be reset to factory settings, all data securely erased and logged as now owned by the terminated user.
- Further access to Bytes Software Services buildings will be as a visitor and they must be escorted.