Information Security Policy

Byrom PLC

Security

Classification: **Public**

1 Introduction

Information is considered a primary asset of Byrom PLC (Byrom) and as such must be protected in a manner equivalent to its value. The confidentiality, integrity and availability of information, in all its forms, are critical to the ongoing functioning and good governance of Byrom. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult to recover.

This policy outlines Byrom's approach to information security management. It provides the guiding principles and responsibilities necessary to protect Byrom's information and assets. Supporting policies, codes of practice, procedures and guidelines will provide further details.

1.1 Policy Statement

Byrom is committed to a robust implementation of information security management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all the physical and electronic information assets for which Byrom is responsible, including those generated by, supplied by or held on behalf of clients, customers and other relevant third parties. The premise for the policy can be stated as:

"Other than information or data defined as public (or unclassified), which is accessible in the public domain, all information, data and assets are only to be accessible on a need-to-know basis to specifically identified, authenticated, and authorised entities."

1.2 Purpose

Protecting information assets is not simply limited to covering electronic data and paper records that Byrom maintains. It also addresses the people who use them, the processes they follow, and the physical hardware used to access them. Therefore, the primary purposes of this policy are to:

- Ensure adequate protection of all Byrom information and information assets (including but not limited to all computers, mobile devices, networks, software, data, physical filing systems and documents) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these, throughout their life cycles.
- Educate Byrom users and vendors about their obligation for the protection of all information and assets and to comply with all relevant UK, EU and Swiss legislations.
- Provide secure working environments for all staff and other authorised users.
- Ensure that all users understand their responsibilities for protecting the confidentiality, integrity and availability of the data they handle.
- Respond to feedback and update as appropriate, initiating a cycle of continuous improvement.

1.3 Scope of the Policy

This policy applies to all Byrom and customer information assets or data that exist in any Byrom processing environment, in any format during any part if its life cycle. The following entities or users are covered by this policy:

- Full or part-time employees of Byrom who have access to Byrom or customer information and/or data.
- Byrom vendors or processors who have access to Byrom or customer information and/or data.
- Other persons, entities, or organisations that have access to Byrom or customer information and/or data.

2 Definitions

Consent

The agreement of a data subject to have his/her personal data processed. Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Database

Any collection of data on more than one legal or natural person, the compilation of which enables data to be obtained on individual data subjects. A database can be either electronic or physical.

Data controller/ holder

The natural or legal person who determines the existence, purpose and contents of a database/collection of data.

Data owner / custodian

The person responsible for the database. The data owner can be a natural person or group of natural persons.

Data processor

The natural or legal person which processes data on behalf of a controller.

Data subject

A natural or legal person about whom data is processed.

DPO (Data Protection Officer)

- Appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices.

- May be a staff member or an external service provider.
- Is provided with appropriate resources to carry out their tasks and maintain their expert knowledge.
- Reports directly to the highest level of management.
- Does not carry out any other tasks that could result in a conflict of interest.

Data transmission

Processing in the form of the transmission of data or databases in any form (written, verbal, electronic or by other means) within a legal person or to third parties.

Disclosure / to disclose

The provision of access to personal data, e.g. through making it available for inspection, transferring it or publishing it.

Encryption

A method that allows information to be hidden so that it cannot be read without special knowledge (such as a password or key).

GDPR (The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679))

Came into effect 25 May 2018, replacing the EU Data Protection Directive (Directive 95/46/EC of the EU Parliament and of the Council of 24 October 1995, on the protection of individuals with regards to the processing of personal data and on the free movement of such data).

ISWG (Information Security Working Group)

An ad-hoc group formed of a member from every Byrom department in order to provide operational input into the development and implementation of information security matters.

Personal data

All information in written, pictorial, acoustic or electronic form which refers to a specific natural or legal person.

Personal data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Personality profile

A collection of data enabling the essential aspects of the personality of a natural person to be assessed. Personality profiles must be treated as sensitive personal data.

Processing / to process

Any handling of data, irrespective of the means and processes used, in particular the procurement, storage, use amendment, disclosure, transmission, archiving or destruction of data.

Pseudonymised / Pseudonymisation

The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Recipient

The addressee of data, irrespective of whether said person belongs to the same legal person as the sender or another.

Sensitive personal data

Data containing information on a person concerning: (i) religious, ideological, political or trade-union-related views or activities; (ii) health, private life or race; (iii) social welfare assistance; (iv) administrative or criminal proceedings and sanctions. Personality profiles are classified as sensitive personal data.

Third parties

Any natural or legal person to whom the data is disclosed or transmitted who does not belong to the same legal person as the sender or recipient (subsidiary companies also count as third parties).

User

Any natural person who is recognised, authorised and granted access to specified data for the purpose of their employment.

3 Information Security Policy

3.1 Principles

The following information security principles provide overarching governance for the security management of information at Byrom.

1. Information will be classified according to an appropriate level of confidentiality, integrity and availability and in accordance with the relevant legislation, regulatory and contractual requirements and Byrom policy.
2. Staff with particular responsibilities for information are responsible for ensuring classification of that information; for handling that information in accordance with its classification level; and for any policies, procedures or systems for meeting those responsibilities.

3. All users covered by the scope of this policy must handle information appropriately and in accordance with its classification level.
4. Information should be both secure and available to those with legitimate needs for access in accordance with its classification level.
5. Information will be protected against unauthorised access and processing in accordance with its classification level.
6. Breaches of this policy must be reported immediately and investigated.

3.2 Legal and Regulatory Obligations

Byrom has a responsibility to abide by and adhere to all UK, EU and Swiss legislation as well as a variety of regulatory and contractual obligations. Additional country specific legislation may also be enforced for specific periods or events. Where a country's data protection laws are less stringent than those of the UK, then the UK's legislation shall be the guiding authority for Byrom activities.

A non-exhaustive summary of the legislation that contributes to content of this policy is provided at Appendix A. Staff are not required to know the various legislation; however, it is the responsibility of the Information Security Manager to ensure that company procedures in line with this policy are fully compliant with the applicable laws, legislations and contracts.

3.3 Information Classification

Byrom have adopted 4 categories of classification, as follows:

3.3.1 Definitions

a. **Confidential**
   This is information that has significant value to Byrom and unauthorised disclosure or dissemination could result in severe financial or reputational damage, including fines, the revocation of contracts and the failure to win bids. Data defined by the UK and Swiss Data Protection Acts as 'Sensitive Personal Data' (e.g. medical records or religious affiliation) falls into this category. Only those who explicitly need access must be granted it and only to the least degree in order to do their work. When such information is held outside of Byrom offices or authorised third party hosts, on mobile devices such as laptops, phones or tablets, or when in transit, it must be protected by suitable encryption technology and/or security protocols.
b. **Restricted**
   This is information where unintended disclosure or dissemination may incur some negative publicity, or some financial or reputational damage to Byrom. Information defined as 'Personal Data' under the UK Data Protection Act is to be regarded as Restricted, as well as any information that could prejudice an individual's security. Restricted information is subject to controls on access, such as only allowing valid logons from a small group of staff. Restricted information must be held in such a manner that prevents unauthorised access i.e. on a system that requires a valid and appropriate user logon before access is granted.

Note: Due to possible financial penalties or losses of contracts, Byrom has decided that single data bases containing 'Personal Data' in excess of 1,000 records are to be classified as Confidential.

c. **Internal**

This is information that the disclosure or dissemination of which is unlikely to cause any lasting financial or reputational harm to Byrom, but could cause some embarrassment, assist competitors or cause distress to employees. Internal information can be disclosed or disseminated by its owner to appropriate Byrom staff and third parties in connection to their work only.

d. **Public / Unclassified**

Public information can be disclosed and disseminated without any restrictions on content, audience or time of publication. Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules. Modification must be limited to individuals who have been explicitly approved and who have authenticated themselves prior to modification.

3.3.2 Summary of Classification

Security Level	Level of Protection	Examples (for the purpose of orientation and guidance only)
Confidential	❖ Make unauthorised access highly unlikely ❖ Ensure actual or attempted compromise will be detected and those responsible identified ❖ Ensure all access attempts are logged, in order to provide an audit trail	❖ Sensitive Personal Data or Personal Data in excess of 1,000 records ❖ Sensitive communications (at discretion of the author or recipient) ❖ UK Border Agency reports / CRB checks ❖ Details that can be used to access company bank accounts ❖ Cash ❖ Staff medical records/reports ❖ Production data bases (subject to content and size) ❖ Client/customer credit cardholder data ❖ Mergers and acquisitions
Restricted	❖ Inhibit casual or wilful unauthorised access ❖ Be likely to help the identification of compromise	❖ Financial records / P&L / Budgets ❖ Experian credit reports ❖ Ongoing contracts and customer agreements ❖ Strategic business plans ❖ Board of Directors minutes / Executive missives ❖ Future travel documents ❖ Traveller profiles/passports ❖ HR records / Personal data of less than 1,000 records ❖ Background checks/ Due diligence reports ❖ Payroll ❖ Pensions ❖ Service agreements ❖ Ongoing proposals / cost assessments ❖ Risk assessments

		❖ IT Source code ❖ System/Server credentials ❖ Technical IT documents ❖ Standard legal documents ❖ Client/customer hotel bookings ❖ Penetration test results
Internal	❖ Promote discretion in order to avoid unauthorised access	❖ Company Policies, guidelines and handbooks ❖ Standard emails (without attachments) ❖ Spent travel documents/ itineraries ❖ Company contact details ❖ Requests for Tender ❖ Office templates ❖ Staff training ❖ De-classified operational data and statistical reports ❖ Customer email addresses ❖ Project planning documents / tools ❖ Old or rejected proposals ❖ Normal staff expenses ❖ Requests for Proposals ❖ Organisational charts ❖ Inspection reports ❖ Operational meeting minutes ❖ Any draft document not held in a higher classification.
Public (Unclassified)	❖ Normal levels to reasonably protect from financial loss caused by theft, loss or damage, or to satisfy insurance requirements.	❖ Information available through the Byrom website or intended for public consumption, including: - Issued press releases - Matters of public record - User guides - Business cards and details thereon - Annual reports - CRM Communications

3.3.3 Information sharing and data transfer

Subject to relevant EU legislation, classified information and data can be shared with or transferred to authorised third parties, subject to the same levels of protection outlined in 3.3.2 above; the methods of transfer are to be in accordance with the classification of the data. Where necessary, non-disclosure agreements or other model contracts are to be signed prior to transfer.

Under the GDPR data subjects may request information about the data held on them. All such requests are to be immediately reported to the DPO and Information Security Manager to ensure compliance; irrespective of which, Byrom is to respond to any such requests within 30 days unless authorised by the DPO. On such occasions if the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information can be transmitted in a commonly used electronic format (unencrypted). When providing any information to the data subject all care must be taken to confirm the identity of the person receiving the data to ensure he/she is the data subject in concerned.

3.4 Processes and Implementation

In order to comply with this policy, the Information Security Manager in conjunction with specific department heads will produce detailed guidance and processes to include, but not be limited to the following:

- IT security procedures
- Physical security procedures
- Training and awareness
- Archiving
- HR/ Employment and Induction processes
- IS Policy audit process

Byrom will only process and store data that is required either by law or that is deemed essential for operational purposes.

3.5 Risk Assessment

Information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals.

In addition, Seamos Marketing has a tool to identify threat and vulnerability intelligence that plays a crucial role in your cybersecurity strategy. This tool focuses on the collection and analysis of advanced intelligence data to identify emerging threats and undetected vulnerabilities in systems. By correlating information from multiple sources of global intelligence, including security reports, vulnerability alerts, and attack trends, the tool provides a comprehensive and anticipated view of risks.

3.6 Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

Byrom reserves the right to monitor activity where it suspects that there has been a breach of policy, under the legislation of The Regulation of Investigatory Powers Act (2000) and the Human Rights Act.

3.7 Accreditation of Information Systems

Byrom shall ensure that all new information systems, applications and networks include a security plan and are approved by the Information Security Working Group (ISWG) before they commence operation.

3.8 Data Backup

Byrom shall ensure that whenever deemed necessary databases will be backed up in a suitable alternative location from the original; subject to EU directives, this can include cloud

technology. Data backups will follow standard best practices to ensure that data can be recovered as and when it becomes necessary.

3.9 Data Retention

Byrom shall only retain data for the minimum period of time that is required by relevant legislation, compliance or until the data has no operational value. If data is to be retained beyond that point for statistical or historical purposes it is to be 'pseudonymized'.

3.10 Compliance, Awareness and Disciplinary Procedures

A breach of this policy could have severe consequences to Byrom, its ability to provide or maintain the integrity, confidentiality, and availability of services. Furthermore, the loss, damage or breach of confidentiality of personal and sensitive personal data is an infringement of the Data Protection Acts (UK and Swiss) as well as the GDPR and may result in criminal or civil actions against Byrom. The loss, damage or breach of confidentiality of contractually assured information may also result in the loss of business or financial penalties against Byrom. Therefore, it is critical that all users of Byrom information systems adhere to this policy and it's supporting policies and guidelines.

Any intentional misuse resulting in a breach of any part of this policy will result in disciplinary action at the discretion of Byrom senior management. Severe, deliberate or repeated breaches of the policy may be considered grounds for summary dismissal; or in the case of a Byrom vendor, termination of their contracted services.

3.11 Incident Handling

It is every user's responsibility to immediately report any actual or suspected breach to this policy, or any activities that could compromise the confidentiality, integrity or availability of Byrom information.

In the first instance reports are to be made to user's immediate line manager and the Information Security Manager. If the breach is in relation to personal data, the matter is to be immediately reported to the DPO. If Byrom are processing personal data on behalf of a controller, any breaches are to be reported to the controller without undue delay, but within 24 hours of discovery. If Byrom are the controller of the persona data, breaches are to be reported by the DPO to the relevant authority within 72 hours or becoming aware of the breach.

Full details of Byrom incident handling are contained in the Byrom Security and Data Protection Incident Management Policy.

3.12 Review and Development

This policy, and any subsidiaries, shall be regularly reviewed by an Information Security Working Group (ISWG) to be convened by the Director of IT and the Information Security Manager. The ISWG will comprise of representatives of all relevant parts of Byrom.

The ISWG will authorise and direct the creation of any specific changes, updates or subsidiary documents in relation to information security and data protection, including payment card security requirements for the protection of card holder information and any related ISO compliance.

Subject to operational commitments, Byrom will review this policy annually. Such reviews will be initiated by the Information Security Manager and include input from the ISWG.

4 Roles and Responsibilities

Staff and Authorised Users

All staff of Byrom, contractors or agency staff working for Byrom, will be regarded as users of Byrom information. This carries with it the responsibility to abide by this policy, its principles and relevant legislation, supporting policies, procedures and guidelines. No individual should have access to information to which they have no legitimate access right. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so.

Data Ownership (Custodians)

In order to classify data, it is necessary that an owner (or custodian) be identified for all data assets. The owner of the information or data is generally the person who generated it and is responsible for classifying their data according to the classification system of this policy. If an owner cannot be determined the Information Security Manager must either nominate an appropriate person or act as its custodian. The Information Security Manager has overall responsibility for developing, implementing and maintaining procedures to identify all data assets and associated owners/custodians. The owner of customer data is the individual who processes it or is assigned ownership of that data.

Heads of Departments

Responsible for the information systems, both manual and electronic that supports their work functions. Heads of departments are to ensure adherence to this policy and report to the Information Security Manager any actual or suspected breaches.

IT Security Manager

Responsible for the technical implementation of IT security and provide advice throughout Byrom on IT security issues.

Security Manager

Responsible for all physical aspects of security and will provide advice throughout Byrom on physical security and threat analysis.

Information Security Manager

Responsible for this and subsequent information security policies and will provide specialist advice throughout Byrom on information security issues.

IT Director

The IT Director of Byrom will be responsible for co-approving the information security policy with the DPO.

Data Protection Officer (DPO)

This position is filled by the Director of Legal of Byrom and will be responsible for overseeing compliance with the GDPR and for co-approving the information security policy with the IT Director.

Appendix A: Summary of Relevant Legislation

The following list of legislation is not exhaustive but provides the basis and authority under which this policy has been established.

- **The Human Rights Act 1998 (United Kingdom)**

Puts the rights set out in the 1953 European Convention on Human Rights into UK law. Article 8, relating to privacy, is of most relevance to information security – it provides a right to respect for an individual's "private and family life, his home and his correspondence", a right that is also embedded within the Data Protection Act.

- **Data Protection Act 1998 (United Kingdom)**

Regulates the use of personal data by organisations. Personal data is defined as information relating to a living, identifiable individual.

The Act is underpinned by eight guiding principles:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to countries outside the EEA without adequate safeguards

- **The (Swiss) Federal Act on Data Protection 1992**

Regulates the use of personal data by organisations.

The Act is underpinned by five guiding principles:

1. Fairly and lawfully processed
2. Processed in good faith and proportionately.
3. Processed for the purpose indicated at the time of collection.
4. The purpose of its processing must be evident to the data subject.
5. If the consent of the data subject is required for the processing of personal data, such consent is valid only if given voluntarily on the provision of adequate information.

Further articles describe matters of security, cross border disclosure and correctness of data.

- **The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)**

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the core principles of data privacy still hold true to the previous EU directive, many changes have been added to the regulatory policies; the key additional points of the GDPR are as follows:

- ***Increased Territorial Scope***. The GDPR applies to all companies processing personal data of data subjects residing in the Union, regardless of the company's location.
- ***Penalties***. Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).
- ***Consent***. Consent to process data must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language
- ***Breach Notification***. Breach notification is mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.
- ***Right to Access***. The data subjects have the right to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in a usable electronic format.
- ***Right to be Forgotten***. Also known as *Data Erasure*, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.
- ***Data Portability***. The right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine-readable format' and have the right to transmit that data to another controller.
- ***Privacy by Design***. The controller shall…*'implement appropriate technical and organisational measures…in an effective way…in order to meet the requirements of*

this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

- ***Data Protection Officers (DPO)***. DPO appointment is mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

- **The EU Data Protection Directive (Directive 95/46/EC of the EU Parliament and of the Council of 24 October 1995, on the protection of individuals with regards to the processing of personal data and on the free movement of such data**).

This Directive applies to data processed by automated means (e.g. a computer database of customers) and data contained in or intended to be part of non-automated filing systems (traditional paper files).

It does not apply to the processing of data:

- by a natural person in the course of purely personal or household activities;
- in the course of an activity which falls outside the scope of Community law, such as operations concerning public security, defence or State security.

The Directive aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down the key criteria for making processing lawful and the principles of data quality.

- **The Computer Misuse Act 1990 (United Kingdom)**

It is intended to deter criminals from using computers to assist in the commission of a criminal offence or from impairing or hindering access to data stored in a computer. The Act contains three criminal offences for computer misuse:

- Unauthorised access to computer material;
- Unauthorised access with intent to commit or facilitate commission of further offences;
- Unauthorised modification of computer material.

- **The Freedom of Information Act 2000 (United Kingdom)**

This gives individuals a right of access to information held by Byrom, subject to a number of exemptions. Requests for information must be made in writing (email, letter or fax) but can be received by any member of staff. Such requests must be responded to within 20 working days.

- **Defamation Act 1996 (United Kingdom)**

Defamation is a false accusation of an offence or a malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organisation's reputation from harm.

- **Terrorism Act 2006 (United Kingdom)**

This act creates a number of offences in relation to terrorism. Section 19 of the Act imposes a duty on organisations to disclose information to the security forces where there is a belief or suspicion of a terrorist offence being committed.

It makes an offence to write, publish or circulate any material that could be seen by anyone to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism.

It also prohibits the writing, publication or circulation of information which is likely to be useful to anyone in the commission or preparation of terrorist acts.

- **Payment Card Institution – Data Security Standards (PCI-DSS)**

These are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data. The standards globally govern all merchants and organizations that store, process or transmit credit card details.

The PCI-DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards.

- **Privacy and Electronic Communications Regulations 20003 (United Kingdom)**

Section 11 of the Data Protection Act allows individuals to control the direct marketing information they receive from organisations. The Privacy and Electronic Communications Regulations specifically regulate the use of electronic communications (email, SMS text, cold calls) as a form of marketing and allow individuals to prevent further contact.

- **Regulation of Investigatory Powers Act (RIPA) 2000 (United Kingdom)**

RIPA regulates the powers of public bodies to carry out surveillance and investigation and also deals with the interception of communications. The Home Office offers guidance and codes of practice relating to RIPA.

- **The Limitations Act 1980 (United Kingdom)**

The Limitation Act is a statute of limitations providing legal timescales within which action may be taken for breaches of the law – for example, six years is the period in which an individual has the opportunity to bring an action for breach of contract.

Other Publications of Reference:

- International Standards Office – ISO/IEC 27000 series (Information security management systems)