YORKSHIRE BUILDING SOCIETY

YORKSHIRE BUILDING SOCIETY

INFORMATION & CYBER SECURITY POLICY OVERVIEW

Updated October 2023

Contents

1. Purpose

The Purpose of the Policy

To support the Society's purpose of 'helping real life happen,' the Information & Cyber Security Policy defines how to protect the confidentiality, integrity and availability of the Society's systems and information.

Failure to effectively manage information & cyber security risks could result in the Society suffering reputational damage or regulatory censure and/or customers, members or suppliers suffering financial loss.

The purpose of the Information & Cyber Security Policy is to build a culture of information & cyber security.

Applicable Regulations and Legislation

The Society is authorised by the Prudential Regulation Authority (PRA) and regulated by the Financial Conduct Authority (FCA).

There are various regulations and legislation that govern how we manage the security of our information. The Society must meet all applicable legal and regulatory requirements. These include, but are not limited to:

- Industry information security standards.
- Financial services regulations.
- Relevant data protection regulations and ICO (Information Commissioner's Office) guidance.
- Fraud and anti-money laundering regulations.

Requirements of the Policy

All colleagues and authorised users are responsible for complying with the Information & Cyber Security Policy.

2. Scope

This policy applies to all Society colleagues, including contingent workers, and all locations they work from.

This policy relates to all information processed by the Society, regardless of how it is processed.

Information takes many forms, and the scope of this Policy includes, but is not limited to:

- All information processed by the Society, regardless of whether it is processed electronically or in paper form, including but not limited to:
  - Personal information (as defined in the Information Management Policy).
  - Operational plans, documents, and records.
  - All information processing facilities used in support of the Society's operational activities to store, process and transmit information.

3. Definitions

- **Authorised Users** – Any colleague, contingent worker, or supplier with approved access.
- **Colleagues** – Permanent Yorkshire Building Society colleagues and colleagues delivering support services to the Society as colleagues of external suppliers.
- **Contingent Workers** - Independent contractors, consultants, or other outsourced and non-permanent workers.

- **Confidentiality** – Information is not made available or disclosed to unauthorised individuals, entities, or processes.
- **Integrity** – Information is complete and accurate.
- **Availability** – Information is available when needed.
- **Information** – Any written, oral or data related information and/or the systems on which information is stored or processed that is of value to the Society, its suppliers, and customers.
- **Information Owner** – An individual accountable for the information asset.
- **Information Processing Facilities** - any equipment, operating systems, or infrastructure that are necessary to facilitate the processing of data completely, accurately, and effectively for example, IT equipment, applications, computer network systems etc.

4. Policy Statements

To support the Society's purpose of helping real life happen, we must maintain the confidence of our customers, colleagues, and regulators by protecting the confidentiality, integrity and availability of the Society's systems and information by implementing the following:

- An information asset register must be established and maintained.
- Information, systems, and processing facilities must be protected against unauthorised or inappropriate access.
- The confidentiality, integrity and availability of information must always be protected in line with its classification, and the risk posed to the Society.
- All networks, systems and software must be securely configured, operated, and maintained.
- An incident response capability must be established and maintained.

5. Implementation and Monitoring

Implementation

The Information & Cyber Security Policy will be published on the Intranet and accompanied by a newsfeed to highlight updates to all colleagues and contractors.

Information Security Risk Management will use various channels to raise awareness such as:

- Annual mandatory training – Delivered to all colleagues and contingent workers though the Learning Portal.
- Ad-hoc awareness activities.
- Regular communications – Delivered via Intranet newsfeeds, articles, and face to face activity.

Understanding of this policy will be assessed via the annual mandatory training module which is completed by all colleagues and contractors.

Monitoring

The Society operates a Three Lines of Defence (3LoD) approach towards risk management. Each LoD has different responsibilities for managing the risk and therefore carries different actions.

The first LoD is directly responsible for the day-to-day management and control of risk throughout the business, generally within business functions. The second line is accountable for competent risk management across the society and overseeing the effectiveness and integrity of the Enterprise Risk Management Framework. The final LoD is providing independent assurance across the first and second LoD through our internal Audit function. Compliance with this Policy will be monitored through the Three Lines of Defence, including:

- Adherence to this policy will be assessed via the Society's Risk & Control Self-Assessment (RCSA) process. The RCSA requires relevant business areas self-certify their adherence to key Society controls.

- Information Security Risk Management will conduct periodic, thematic reviews and risk assessments on key controls or systems to confirm compliance with the Information & Cyber Security Policy and associated standards and policy guides. Any risks found as a result of these activities will be managed following the Society's Enterprise Risk Management Framework.

- Information Security Risk Management will conduct regular compliance reviews to ensure the Society is compliant with industry security standards such as Payment Card Industry Data Security Standard (PCI-DSS) and LINK Scheme Information Security Standard.

- Regular management information concerning the operation of information & cyber security controls will be given to Board.

- Internal Audit supplies independent assurance on the Society's internal controls to the Board's Audit Committee, using a risk-based approach in defining its audit plan. This activity includes performing a risk assessment of the audit universe (i.e., all the business areas and risks that could be audited given unlimited resources) including information & cyber security risk. Internal Audit supplements its own resources with external specialist resources as needed.

Any instances of non-compliance, actual or suspected must be reported to the Information Security Risk Management team.

6. Approval

The Group Risk Committee is responsible for approving the policy.

The Information & Cyber Security Policy is reviewed and re-approved annually.