Yorkshire Building Society

Information Security Policy Overview

Contents

YORKSHIRE BUILDING SOCIETY

1. Purpose

The Purpose of the Policy

The trust of both customers and colleagues is at the very heart of our vision to become the most trusted provider of financial services in the UK.

The purpose of the Information Security Policy is to protect the confidentiality, integrity and availability of the Society's Information Assets.

Applicable Regulations and Legislation

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

The Society has a duty to comply with the following applicable regulations and legislation;

- Computer Misuse Act
- Data Protection Regulation 2018 (GDPR)
- Privacy and Electronic Communications Regulations 2003
- The Fraud Act
- Financial Conduct Authority Regulations
- Prudential Regulation Authority Regulations
- Payment Card Industry Data Security Standard
- LINK Security Standards
- BACS Cash ISA Transfer of Conduct
- Payment Services Directive 2

Requirements of the Policy

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

2. Scope

This policy applies to all Society colleagues including contingent workers and all locations that they operate 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 Information Security 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:
  - Customer information
  - Operational plans, documents and records
  - Colleague records
- All information processing facilities used in support of the Society's operational activities to store, process and transmit information

3. Definitions

- **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 Assets** – 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.
- **Authorised Users** – Any colleague, contingent worker or supplier with approved access.

- **Colleagues** – Permanent YBS 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.
- **LINK Scheme** - A network which connects the UK's cash machines and provides consumers with universal access to their cash.
- The BACS cash ISA Transfer of Conduct - The Guide & Rules for the Bacs Cash ISA Transfer service require that on an annual basis YBSG certifies their compliance to the scheme's Code of Conduct.
-

4. Policy Statements

- Unauthorised use of information assets and information processing facilities must be prohibited, and all Information Assets must be protected against unauthorised access or use in line with this policy and the above related standards.
- Information Assets must be recorded on a register to enable the Society to fully understand what information it holds in order to protect it.
- The confidentiality of Information Assets must be maintained and protected from unauthorised disclosure in order to safeguard customers, colleagues and suppliers to prevent the Society suffering financial loss, reputational damage or regulatory censure.
- Integrity of information must be maintained. Information must be complete and accurate, all systems, assets and networks must operate correctly according to specifications.
- All Information Assets required for operational activities must have minimum recovery times specified, with defined availability requirements which must be met.
- Statutory, regulatory and contractual obligations in relation to Information Assets must be met.
- Business continuity plans must be produced, maintained and tested.
- Suppliers with access to Society sites, systems or Information Assets must be reviewed by the Information Security Risk team.
- The Society must establish an incident response capability so that the organisation is ready to respond to incidents. The plan must contain key elements to allow the Society to respond effectively in the event of a breach that puts the confidentiality, integrity or availability of the Society's assets at risk.

5. Implementation and Monitoring

Implementation

The Information Security Policy is available to all colleagues on the Intranet.

The Information Security Risk Team will use various channels to raise awareness such as;

- **Annual mandatory training** – Delivered to all colleagues and contingent workers though the Learning Portal.
- **Awareness presentations** – Delivered in colleague connect sessions.
- **Regular communications** - Delivered via TV screens, Intranet articles and face to face activity.

Understanding of this policy will be assessed via the annual mandatory training module.

Monitoring

The Society operates a Three Lines of Defence (LoD) 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:

- The Risk and Control Self-Assessment (RCSA) process;
- Conducting periodic, thematic reviews and risk assessments on key controls or systems to identify non-compliance with the Information Security Policy and associated policy guide/standards. Any risks identified will be managed through the Group's Risk Management Framework.
- Regular compliance reviews to ensure the Society is compliant with the industry security standards such as Payment Card Industry Data Security Standard and LINK Scheme Information Security Standard.

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

6. Approval

The Information Security Policy will be reviewed annually by the Information Security Risk Team and submitted to the Society Risk Committee for approval.

The Customer Services Divisional Risk Committee oversees changes to the Policy.