holibob

Trust Holibob - High-level Information Security Policy

Version: 15

15 March 2024

Table of Contents

1 Introduction

This document details the measures taken by Holibob (The Company) to secure the information we are entrusted with and comply with local and international laws regarding different data classifications.

1.1 Purpose

Information collected, analysed, stored, communicated, and reported upon may be subject to theft, misuse, loss, and corruption. Poor education and training and the breach of security controls may also put information at risk.

Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation, and possible judgements against The Company.

This high-level Information Security Policy sits alongside our "Information Risk Management Policy" and "Data Protection Policy" to provide a high-level outline of and justification for our risk-based information security controls.

1.2 Objectives

The company's security objectives are that:

- Our information risks are identified, managed and treated according to an agreed risk tolerance.
- Our authorised users can securely access and share information to perform their roles.
- Our physical, procedural and technical controls balance user experience and security.
- Our contractual and legal obligations relating to information security are met.
- Our teaching, research, and administrative activities consider information security.
- Individuals accessing our information are aware of their information security responsibilities.
- Incidents affecting our information assets are resolved and learnt from to improve our controls.

1.3 Scope

Our Information Security Policy and its supporting controls, processes and procedures apply to all information used at Holibob in all formats. This includes information processed by other organisations in their dealings with us.

The Information Security Policy and its supporting controls, processes, and procedures apply to all employees, consultants, and contractors who access our information and technologies, including external parties providing information processing services to us.

1.4 Compliance monitoring

Compliance with the controls in this policy will be monitored by the Information Security Team and reported to the Information Governance Board.

1.5 Review

The Chief Information and Security Officer will review this policy annually and as required by changes in systems, organizational structure, or policy.

1.6 Policy Statement

It is our policy to ensure that information is protected from a loss of:

- Confidentiality – information will be accessible only to authorised individuals.
- Integrity – the accuracy and completeness of information will be maintained.
- Availability – information will be accessible to authorised users and processes when required.

The company will implement an Information Security Management System based on certified standards as required. The Company will be mindful of the approaches adopted by all stakeholders.

The Company will adopt a risk-based approach to the application of the following controls:

1.6.1 Information security policies

The company maintains and implements a set of lower-level controls, processes, and procedures for information security to support the high-level Information Security Policy and its stated objectives.

The Chief Information and Security Officer will control and approve this suite of supporting documentation, which will be published and communicated to all stakeholders.

1.6.2 Organisation of information security

The company maintains and implements suitable governance arrangements for information security management. This will include identifying and allocating security responsibilities to initiate and control the implementation and operation of information security across the company.

The company maintains:

- An executive to chair to the Information Governance Board and take accountability for information risk.
- An Information Governance Board to influence, oversee and promote the effective management of our information.
- An Information Security specialist to manage the day-to-day information security function.
- Information Asset Owners (IAOs) to assume local accountability for information management.
- Information Asset Managers (IAMs) responsible for day-to-day information management.

1.6.3 Human resources security

Our security policies and expectations for acceptable use will be regularly communicated to all users to ensure they understand their responsibilities.

Information security education and training will be made available to all staff. Poor or inappropriate behaviour will be addressed and may lead to disciplinary actions.

Security responsibilities will be included in role descriptions, person specifications and personal development plans where practical.

1.6.4 Asset management

All assets will be documented and accounted for.

This includes:

- Information
- Software
- Electronic information processing equipment, including:
    - Workstations

    - Laptops
    - Servers
    - Cloud infrastructure
    - 3rd Party cloud software
- Service utilities
- People including
    - Employees
    - Contractors
    - Consultants

All assets will have owners who will be identified and responsible for maintenance and protection.

All information assets will be classified according to their legal requirements, business value, criticality and sensitivity. Classification will indicate appropriate handling requirements. All information assets will have a defined retention and disposal schedule.

1.6.5 Access control

Access to all information is controlled and driven by business requirements based on least privilege access. Users will be granted access or have arrangements made according to their role and the information classification only to a level that will allow them to carry out their duties.

A formal procedure is maintained and followed for granting and revoking access to all information systems. This includes mandatory authentication methods based on the sensitivity of the information being accessed and will include consideration of multiple factors as appropriate.

Specific controls will be implemented for users with elevated privileges to reduce the risk of negligent or deliberate system misuse. The separation of duties will be implemented where practical.

1.6.6 Cryptography

The Company provides guidance and tools to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information and systems.

1.6.7 Physical and environmental security

The company operates 100% remotely and has no permanent physical office space.

The company does not have dedicated server facilities and instead uses Infrastructure as a Service (IaaS) provided by Amazon Web Services (AWS) and other mainstream cloud providers.

1.6.7.1 In-person meetings

When company members meet in person, they generally do so in shared office facilities such as WeWork. The company takes advantage of the access controls provided by such operators, and only invited persons are granted access.

1.6.7.2 Information Processing

Information processing occurs within our dedicated software, which operates within the infrastructure of our cloud infrastructure providers and in the cloud-hosted Software as a Service (SaaS) applications we use.

Strong controls are in place to manage access to all such systems as described in the suite of documentation that this document introduces.

1.6.8 Operations security

The company maintains and implements policies to ensure the secure operation of information processing systems.

This includes:

- Documented operating procedures
- RunBooks for critical incident response
- Documented and tested disaster recovery procedures

- Formal change management
- Controls against malware
- Defined use of logging, observability and events with long-term glacial storage
- Vulnerability management

1.6.9 Network and egress security

The company maintains and implements network security controls to protect information within its networks.

The company provides tools and guidance to secure information transfer within its networks and with external entities. This aligns with the classification and handling requirements associated with that information.

1.6.10 Communications security

The company maintains and implements policies for the security of the email, including the use of DMARC compliance, malware checking, labelling of email sources and checking of all links and attachments embedded in the emails.

The company guides employees on the appropriate use of email and other communication tools and provides awareness training on phishing and other common techniques bad actors use.

1.6.11 System acquisition, development and maintenance

Information security requirements are defined during the development of business requirements for new information systems or changes to existing information systems.

Controls to reduce any risks identified will be implemented and maintained where appropriate.

Systems development is subject to strict risk-based change control and separation of test, development and operational environments.

1.6.12 Partner and other stakeholder relationships

The company's information security requirements are considered when establishing relationships with Partners, Suppliers and other stakeholders, to ensure that assets accessible to and provided by stakeholders are protected in accordance with policy.

Stakeholder engagements and monitored and audited according to the value of the assets and the associated risks.

1.6.13 Critical incident management

Guidance is given on what constitutes a critical information security incident and how to report it.

Actual or suspected breaches of information security must be reported and investigated. The appropriate action to correct the breach will be taken, and any learning will be built into controls.

1.6.14 Business continuity management

The company maintains, implements and rehearses arrangements to protect critical business processes from the effects of major failures of information systems or disasters. This ensures timely recovery from business disruptions in line with documented business needs.

This includes:

- Regularly monitored an encrypted backup of all information to secure storage that is separate from the operational infrastructure
- Built-in resilience within the software architecture and supporting infrastructure of operational systems
- Business continuity plans that are maintained and tested in support of this policy.

Business impact analysis is undertaken, detailing the consequences of:

- Disasters impacting the operational efficiency of Employees or Systems
- Security failures
- Loss of 3rd party provided services

1.6.15 Compliance

The company ensures that information systems' design, operation, use, and management comply with all statutory, regulatory, and contractual security requirements.

Currently, this includes:

- Data protection legislation in multiple jurisdictions, such as GDPR
- The payment card industry standard (PCI-DSS)
- The company's contractual commitments

The company uses a combination of internal and external audits to demonstrate compliance against chosen standards and best practices.

This will include:

- IT health checks
- Gap analyses against documented standards
- Internal checks on staff compliance
- Returns from Information Asset Owners