Employee Passport

Your people. Verified. Accountable.

Information Security Policy

Document Information

Owner	Daniel Sayers
Approver	Mark Whitfield
Last Review Date	05/3/2026
Next Review Date	
Related ISO clauses	5.1
Related Annex A clauses	5.2, 8.13
Classification	Confidential

Definitions

Information Security

Employee Passport defines information security as the policies, procedures, and controls implemented to protect the confidentiality, integrity, and availability of information assets.

CIA

CIA is an acronym that stands for Confidentiality, Integrity, and Availability. These three terms are the pillars of information security, and the purpose of Employee Passport's ISMS is to ensure that all information assets within the scope of the ISMS are protected in respect of these three pillars.

- Confidentiality - Ensuring that information assets can only be viewed by those who need to view them.
- Integrity - Ensuring that information assets remain in their original form or can only be changed by relevant people out of necessity.
- Availability - Ensuring that information assets are available to whoever needs them, whenever they are needed.

Information Assets

Information assets are pieces of information or things that process information that hold value to the organisation. Information assets include:

- Data
- Hardware
- Software
- Services
- Locations
- People

ISMS

ISMS stands for Information Security Management System, and is the collection of policies, procedures, and controls within the ISMS' scope.

Policies, Procedures, and Controls

- Policies – High level statements of intent of the organisation regarding information security.
- Procedures – Formal instructions on completing specific information security tasks.
- Controls – Specific organisational, people, physical, or technological measures put in place to protect information assets and mitigate or avoid risks.

Incident

An incident within the ISMS' scope refers to any circumstances where the CIA of information assets is affected.

Risk

A risk is a deviation from an expected outcome with a negative impact on objectives.

Non-conformity

A non-conformity is a failure to meet a mandatory requirement of the ISO 27001 standard.

Interested Parties

The people, groups, or organisations that either impact or are impacted by Employee Passport. These parties are defined in the Context of the Organisation document.

Employee Passport

Your people. Verified. Accountable.

Scope

These measures apply to all people, devices, systems, processes, geographic locations, and cloud services (information assets) under the organisation's control as defined in the scope in the Context of the Organisation document, complete with exclusions established in the same document.

Objectives

The ISMS addresses the following objectives:

- The need to comply with regulation, legislation, and contractual agreements
- Compliance with standards, including ISO 27001 and Cyber Essentials
- Build trust with clients and users
- Support business objectives

Further information on these objectives can be found in the Context of the Organisation document.

Failure to safeguard the CIA of information assets within the organisation can lead to disruption to business activities and operations, endanger data, and result in legal and regulatory penalties.

Employee Passport is committed to safeguarding the CIA of information assets within its scope.

The Information Security policy is available and communicated within the organisation, with an external version available to interested parties as appropriate.

Principles

Employee Passport adheres to several well-known principles to guide its information security policy:

- Secure by design – Implementing security into project management and development processes.
- Risk-based approach – Implementing policies, procedures and controls with the aim of reducing identified risks.
- Principle of Least Privilege – Ensuring that all employees, contractors, and third parties access information assets based purely on business need.

- Compliance – Ensuring that Employee Passport and its employees operate in accordance with legislation, regulations, and contractual agreements.
- Continuous improvement – maintaining information security by constantly assessing the performance of the ISMS and improving it whenever possible.

Policies

The ISMS contains topic specific policies, listed below:

- Acceptable use of Assets Policy
- Backup Policy
- Clear Desk and Clear Screen Policy
- Cloud Services Policy
- Cryptographic Controls Policy
- Data Retention Policy
- Firewall and Network Security Policy
- Incident Response Policy
- Information and Classification Handling Policy
- Information Transfer Policy
- Malware Protection Policy
- Mobile Devices and Teleworking Policy
- Password Policy
- Physical and Environmental Security Policy
- Privacy and Protection of Personally Identifiable Information Policy
- Secure Configuration Policy
- Secure Development Policy
- Secure Disposal Policy
- Supplier Relationships Policy
- Technical Vulnerability Management Policy
- User Access Control Policy

Roles and Responsibilities

Employee Passport defines three roles for the implementation, evaluation, and improvement of its ISMS:

Role	Assigned person	Contact information

Your people. Verified. Accountable.

Top Management	Mark Whitfield (Co-Owner)	mark@epl-hub.com
Information Security Officer	Daniel Sayers (Junior Cyber Operations Associate)	dan@employeepassporthub.com
Management Review Team	Top Management Information Security Officer	

These roles contain several responsibilities, listed below:

Top Management:

- Demonstrate leadership and commitment with respect to the ISMS by:
    1. Ensuring the Information Security Policy and Objectives are established and compatible with the strategic direction of the organisation
    2. Ensuring the integration of the ISMS requirements into the organisation's processes
    3. Ensuring that the resources needed for the ISMS are available
    4. Communicating the importance of effective information security management, and of conforming to the ISMS requirements
    5. Ensuring that the ISMS achieves its intended outcome
    6. Directing and supporting persons to contribute to the effectiveness of the ISMS
    7. Promoting continual improvement
    8. Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility
    9. Assignment of the Information Security Officer role, and provision of ongoing support to the role to achieve information security objectives
- Establish an Information Security policy that:
    1. Is appropriate for the purpose of the organisation
    2. Includes information security objectives
    3. Includes a commitment to satisfy requirements related to information security
    4. Includes a commitment to continual improvement of the ISMS

- Ensuring the assignment of the Information Security Officer role

Information Security Officer:

- Creating, implementing, and communicating the Information Security policy as well as topic specific policies
- Creating, implementing, and communicating ISMS procedures to all relevant staff
- Assessing, analysing, and treating information security risks to the organisation
- Implementing relevant ISO 27001 controls from Annex A as defined in the Statement of Applicability to treat information security risks
- Monitoring the ISMS for non-conformities
- Evaluating the ISMS for opportunities for improvement
- Ensuring that the ISMS conforms to the requirements of ISO 27001
- Reporting on the performance of the ISMS to top management

Management Review Team:

- Conduct reviews of the ISMS and agree on changes to it in response to annual reviews or recent major incidents.

All employees, contractors, and third parties are required to adhere to the ISMS' established policies, procedures, and controls, and report incidents.

Compliance and Enforcement

Compliance with this policy will be monitored, with scheduled audits occurring annually or following a major information security incident. Violations of this policy will be dealt with in accordance with Employee Passport standard disciplinary procedures, which may include a requirement for re-training in certain ISMS policies, procedures, or controls.

This policy enables compliance with ISO 27001.

Review

This policy is reviewed and updated by the Information Security Officer and approved by the Management Review Team annually or in the event of a major incident.

Employee Passport

Your people. Verified. Accountable.

Change Control Table

Version	Date	Author	Summary of Changes	Approved by	Approval Date
1.0	05/03/2026	Daniel Sayers	Document created	Mark Whitfield	05/03/2026