Information Security Policy

Scope

This policy applies to all Jobs 22 colleagues.

Purpose

- To communicate the Executive's commitment to protecting the confidentiality, integrity and availability of the organisations' information assets.
- To set out the strategic direction for the management of information security.
- To specify the implementation of an Information Security Management System (ISMS) and to maintain Certification of that ISMS to ISO27001:2022.
- To maintain CyberEssentials Plus Certification.
- To serve as the overarching policy from which the framework of policies, procedures, and records that form the ISMS derive.
- To promote a risk based approach into the organisation's culture.
- To set out the organisations' information security objectives.

The Policy

- Department Heads are committed to ensuring all information assets held, stored or processed, including those processed on Jobs 22's behalf by a third party, are securely protected against unauthorised access, disclosure, alteration or loss in accordance with legal, regulatory and contractual obligations.
- Jobs 22's information security management and processes are aligned with and support the aims and objectives set out in strategic business plans. Information related risks will be identified, assessed and mitigated through risk assessments, risk treatment plans and a register of security controls known as the Statement of Applicability.
- The organisation's commitment to, and management of, information security is governed by the Information Security Steering Group (ISSG) which meets quarterly. The ISSG is chaired by the IT Director and the Group provides overarching governance for information security and data protection and comprises senior management representatives from key departments. An annual Management Review is held with representatives from the ISSG and to which the Chief Executive Officer is a standing invitee.
- The Chief Executive Officer acts as the Senior Information Risk Owner but has delegated his responsibilities as SIRO to the Business Improvement Director, with the exception of Board representation.

Objectives

1. To maintain ISO27001:2022 Certification.
2. To demonstrate continual improvement by the ongoing evaluation and review of our effectiveness measurements and addressing identified areas for improvement.
3. To take account of feedback from interested parties to support the drive for continual improvement.
4. To maintain CyberEssentials Plus Certification.
5. To ensure the organisation fulfils its legal, regulatory and contractual responsibilities under Data Protection and other relevant Legislation.

6. To ensure information security is embedded throughout the organisation and is taken account of in all established management frameworks, strategic aims and objectives and organisational process and practice.
7. To preserve the confidentiality, integrity and availability of all information assets. This will be achieved by:
   a. Determining and documenting the processes into which information security should be integrated across all functions of the organisation.
   b. Ensuring that all users who access Jobs 22's ICT system and/or premises are aware of their security responsibilities.
   c. Ensuring that all information and associated assets are accessible to authorised users when required and that information is only accessible to those authorised and to prevent unauthorised access to Jobs 22's information, intellectual property and information processing assets.
   d. Ensuring that safeguards are in place to protect the accuracy and completeness of information and to prevent deliberate or accidental, partial or complete, destruction or unauthorised modification of data or any other information asset.
8. To ensure a risk based approach underpins all strategic decision making and that privacy and information security issues and risks are identified, assessed and managed as part of this decision making process.
9. To ensure the organisation implements and maintains a fully integrated records management process which meets its legal and contractual obligations and assigns responsibility for facilitating the timely disposal/deletion of all records.
10. To ensure performance against these objectives forms part of the Effectiveness Measurement monitoring by the ISSG.

Owner and Approval

The Chief Executive Officer is the owner of this document and is responsible for ensuring that this policy is reviewed at least annually.

The current version of this document is available to all colleagues on the corporate intranet. The policy is published on the Jobs 22 website making it available to interested parties.

The Information Security Policy was first approved by the IT Director and is issued on a version controlled basis under the signature of the Chief Executive Officer.

Signed by: Date: 21/06/2023

Ayden Sims
Chief Executive Officer

The Information Security Manager is the author of this document and is responsible for ensuring that this policy is reviewed at least annually.

A current version of this document is available to all colleagues on the corporate intranet.

This document was approved for publication by the IT Director and is issued on a version controlled basis.

Document Management:

ELT Owner	Chief Executive Officer
Policy Author:	Information Security Manager
Effective Date:	22/06/2021
Review Date:	20/06/2024
Document reference:	IS5.1 Information Security Policy

Change History Record

Version control	Substantive change narrative	Author of substantive change	Date of substantive change
0.01	First draft of policy incorporating current employment contract clauses	Information Security Team	16/06/2021
1.0	Approved for publication by the IT Director	Information Security Team	22/06/2021
2.0	Policy reviewed and minor amendments made. Objectives remain as previous.	Information Security Team	20/06/2022
3.0	Policy reviewed and objectives updated. Also included reference to this policy being available on Jobs 22 website.	Information Security Team	21/06/2023

Equality Statement

Jobs 22 is committed to promoting the equality of opportunity for all of our staff and service users, and for ensuring that our staff and beneficiaries do not feel discriminated against, harassed or victimised by our working practices, whether they share a protected characteristic or not. With this in mind, allowances can and will be made wherever reasonable and practicable to any of the rules and conditions outlined within this policy if it is determined that any individual or group is negatively impacted by one or more of these rules and conditions.

If you feel that this policy is discriminatory in any way, or that your personal circumstances are such that adjustments to the conditions of the policy are required for you, then you are encouraged to speak with your line manager at the earliest opportunity, and/or to contact the executive lead for this policy. Any issues raised will be treated without prejudice and in the strictest confidence.

Annex 1: Equality Impact Assessment

Jobs 22 is committed to always avoiding the potential for unlawful discrimination, harassment and victimisation; advancing equality of opportunity between people who share a protected characteristic and those who do not; and, foster good relations between people who share a protected characteristic and those who do not.

An Equality Impact Assessment (EIA) is a tool for identifying whether or not strategies, projects, services, guidance, practices or policies have an adverse or positive impact on a particular group of people or equality group. While currently only public bodies are legally required to complete EIA's, Jobs 22 has adopted the process in line with its commitment to continually improve our equality performance.

Summary

This EIA is for:	Information Security Policy
EIA completed by:	Information Security Manager
Date of Assessment:	16/06/2021
Assessment Approved by:	

Objectives and intended outcomes
This EIA has been completed in order to ensure that the implications and potential impact, positive and negative, of the Information Security Policy for all staff have been fully considered and addressed, whether or not the staff members share a protected characteristic.

Potential Impacts, positive and negative

Equality Area	Positive	Neutral	Negative	Summary
Age	☐	☒	☐	The policy applies equally to all members of staff regardless of age. It's not considered that the policy includes any guidance or rules that may impact either positively or negatively on any member of staff because of their age.
Disability	☐	☒	☐	The policy applies equally to all members of

				staff regardless of disability. It's not considered that the policy includes any guidance or rules that may impact either positively or negatively on any member of staff because of their disability.
Pregnancy and Maternity/Paternity	☐	☒	☐	It's not considered that the policy positive or negatively impacts on pregnant women or on staff on maternity or paternity.
Race (including origin, colour and nationality)	☐	☒	☐	The policy applies equally to all members of staff regardless of their race, origin, colour or nationality. It's not considered that the policy includes any guidance or rules that may impact either positively or negatively in these respects.
Gender and Gender Reassignment	☐	☒	☐	The policy applies equally to all members of staff regardless of their gender at any given time. It's not considered that the policy includes any guidance or rules that may impact either positively or negatively on any member of staff because gender.
Sexual Orientation	☐	☒	☐	The policy applies equally to all members of staff regardless of their sexual orientation. It's not considered that the policy includes any guidance or rules that may impact either positively or negatively on any member of staff because their sexual orientation

Negative Impacts and Mitigations

Negative Impact	Mitigation	Owner
None		