PixelFusion

People Security Policy

Document Control

Organisation Name	Pixel Fusion Limited
Document Name	People Security Policy
Version	V1

Document Revision History

Date	Version	Changed By	Details of Change
12/11/2025	DRAFT	Alice Ward	Policy draft
01/12/2025	1	Gareth Heggie	Approved

Statement of Applicability Controls

ISO 27001

Control Reference	Control Heading
6.1	Screening
6.2	Terms and Conditions of Employment
6.3	Information Security Awareness, Education, and Training
6.4	Disciplinary Process
6.5	Responsibilities After Termination of Change of Employment
6.6	Confidentiality or Non-Disclosure Agreements

Contents

1. Purpose 4
2. Scope 4
3. People Security Policy 4
3.1. Screening 4
3.2. Terms and Conditions of Employment 5
3.3. Information Security Awareness, Training and Education 5
3.4. Disciplinary Process 5
3.5. Responsibilities after Termination or Change of Employment 6
3.6. Confidentiality and Non-Disclosure Agreements 7
4. Policy Compliance 8
4.1. Compliance Measurement 8
4.2. Exceptions 8
4.3. Non-Compliance 8
4.4. Continual Improvement 8

1. Purpose

- The purpose of this policy is to ensure information security and confidentiality is maintained throughout the employment lifecycle.

2. Scope

- All full-time employees, contract workers, consultants, part-time staff, temporary workers, and other personnel.

3. People Security Policy

3.1. Screening

- Screening and background checks are conducted on all candidates for full-time, part time, and temporary roles before employment.

- The following checks are carried out in line with the **Joiner, Mover, Leaver Procedure** with appropriate copies to be taken and maintained on the individuals HR file:

    - Obtaining appropriate references;
    - Verification of the applicant's CV;
    - Confirmation of the Right to Work in the UK;
    - Confirmation of relevant academic and professional qualifications;
    - Disclosure and Barring Service (DBS) Check.

- Occasionally we will also need to seek verification from external parties to check the information provided by the candidate. Where such a situation arises, we will first request written permission from the candidate.

- All checks are performed in accordance with relevant laws, regulations, ethics, and are proportional to our requirements, the classification of the information being accessed, and the perceived risk.

- Where individuals are contracted through the supply of services, the **Supplier Management Policy** should be followed.

- If the results of screening and verification checks adversely affect the hiring decision, the candidate will be advised accordingly.

- Where a candidate is hired for a specific information security role, we ensure the candidate has the necessary competence to perform the security role.

3.2. Terms and Conditions of Employment

- Contractual obligations for employees should include:
    - Appropriate confidentiality clauses; and
    - Actions to be taken if personnel disregard our information security and privacy policies.
- We ensure employees understand their own, and the organisation's responsibilities for information security and privacy through providing appropriate awareness, education, and training as detailed below.

3.3. Information Security Awareness, Training and Education

- All employees receive appropriate awareness, education and training.
- Upon induction, every employee is required to complete a basic level of training.
- This training is refreshed at least annually.
- We perform ongoing phishing simulation training for all employees.

3.4. Disciplinary Process

- Where a confirmed policy offence has taken place, the **Disciplinary Procedure** should be followed.
- When determining the action to be taken, the following will be considered:
    - The nature and severity of the offence, and its consequences.
    - Whether the offence was intentional (malicious) or unintentional (accidental).
    - Whether or not this is a first time, or a repeat offence; and
    - Whether or not the offender was appropriately trained.

3.5. Responsibilities after Termination or Change of Employment

- Following the end of employment, the **Joiner, Mover, Leaver Procedure** will be followed.

- Leavers will be reminded about their ongoing responsibilities relating to confidentiality.

- Ongoing responsibilities may include any additional responsibilities and, where appropriate, and additional confidentiality agreements.

- Where appointed third parties are terminated, the **Supplier Management Policy** will be followed.

3.6. Change of Employment Responsibilities

- Where there is a material change in employment responsibilities, the **Joiner, Mover, Leaver Procedure** will be followed.

3.7. Specialist Roles and Responsibilities

- Those with specific information security and privacy responsibilities are identified within the **Roles and Responsibility Register**.

    - The information security and privacy role and responsibility of any individual who leaves, or changes job roles will be both identified and transferred to another appropriate individual.

    - Where changes are made to personnel and operating arrangements regarding information security and privacy, the necessary contractors / employees will be informed.

3.8. Confidentiality and Non-Disclosure Agreements

- All confidentiality clauses within contracts and agreements or non-disclosure agreements (NDAs) shall be legally enforceable.

- The terms within the agreements are determined by taking into account the type of information that will be handled, its classification level, its use, and the permissible access by the receiving party.

- Where third parties will have access to information, the **Supplier Relationship Policy** will be followed.

- Where an employee is provided with additional sensitive information, it may be required for them to sign an additional NDA, specific to that information.

- Where required to do so, the following will be considered for inclusion within the NDA:

    - A definition of the information to be protected.

    - The expected duration of an agreement, including cases where it can be necessary to maintain confidentiality indefinitely or until the information becomes publicly available.

    - The required actions when an agreement is terminated.

    - The responsibilities and actions of signatories to avoid unauthorised information disclosure.

    - The ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information.

    - The permitted use of confidential information and rights of the signatory to use said information.

    - The right to audit and monitor activities that involve confidential information for highly sensitive circumstances.

    - The process for notification and reporting of unauthorised disclosure or confidential information leakage.

    - The terms for information to be returned or destroyed at agreement termination.

    - The expected actions to be taken in the case of non-compliance with the agreement.

- The requirements for confidentiality and non-disclosure agreements will be reviewed on an ongoing basis and where any change occurs that may impact these requirements.

4. Policy Compliance

4.1. Compliance Measurement

- The Information Security Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

- Any exception to the policy must be approved and recorded by the Information Security Team in advance.

4.3. Non-Compliance

- Security breaches by employees relating to the ISMS may be treated as misconduct as per the **Disciplinary Procedure** and serious breaches may lead to dismissal.

4.4. Continual Improvement

- This policy is updated and reviewed as part of the continual improvement process.