1. Purpose

The purpose of this policy is to inform EWR Co. employees of the risks associated with information security that the organisation is prepared to accept, to ensure that risk management is an integral, visible and consistent part of routine management activity across EWR Co., and provide a framework to define EWR Co.'s information risk appetite for its various Information Assets. It covers risk awareness, ensuring that personnel understand and accept risk in the context of EWR Co.'s aims and objectives, and can understand and work within EWR Co.'s established risk appetite.

This Policy covers risk associated with all information within EWR Co. This relates to (but is not limited to) information held in the following formats:

- Customer / client / service user.
- Staff and personnel.
- Organisational, business, commercial and operational
- Research, audit, and reporting

This Policy applies to all those working for EWR Co. in whatever capacity, including employees, volunteers, students, temporary workers, contractors, suppliers and Third Parties (hereafter referred to as 'employees'). Third Parties and Suppliers are expected to follow this approach unless specifically excluded or where conditions have been applied within the procurement and contract management process. This policy is particularly relevant to Information Asset Owners (IAOs), and the SIRO (Senior Information Risk Owner).

Employees may be subject to disciplinary action if they fail to adhere to any of the governance laid out in this policy. Unlawful or illegal conduct may result in separate criminal or civil proceedings.

2. Policy

Ultimately, our primary concern for information security is the preservation of Confidentiality, Integrity, and Availability (The CIA Triad):

- **Confidentiality:** Data is only accessible by authorised personnel.
- **Integrity:** Data is accurate and has not been altered.
- **Availability:** Data is always available to those that need it.

EWR employees will always:

- Ensure that all Information Assets (IAs) have proportionate controls in place that allow them to be fully exploited whilst managing the risks.
- Ensure that IAs that are Business-Critical (BCIAs) are individually identified, recorded and managed in accordance with the Information Governance Policy.
- Be aware of how to classify external and internal threats to EWR. This is in accordance with guidance found in EWR's Risk Management Procedure.
- Contact the relevant IAO should any risks to Information security be identified.
- Ensure that all documents, including physical and digital documents, are classified in accordance with the official government guidelines where appropriate. These guidelines can be found here.
- Always understand what Information Assets and Business-Critical Information assets are. This information can be found in the Information Governance Procedure.

EWR will always:

- Assign by default the role of Information Asset Owner to the Senior Leadership Team..
- Allow IAOs to delegate their responsibility to one individual as described in the Information Governance Procedure.
- Ensure that IAO Forums are held on a quarterly basis. This is covered in more detail in the Information Governance Procedure.

The SIRO and IAOs:

- Agree that they have read, understood, and will following the guidance and responsibilities laid out in the Information Governance Policy.

The IT Department will always:

- Ensure that a Cyber Security Threat Assessment is conducted against EWR on an regular basis.
- Follow a Threat Assessment with a Threat Modelling exercise to ensure that the outputs of the Threat Assessment is properly understood and applied to our risk management approach. More information can be found in the IT Security Management Procedure.
- Review IT risks with the Risk Team on a monthly basis.

The IT Team will regularly conduct Risk Assessment. Risk Assessments will always be conducted:

- As part of the IT Change Process, and ensure that any identified risks are dealt with appropriately, in-line with the Risk Management Procedure.
- Outside of the IT Change Process, to ensure work conducted in BAU is assessed, and identified risks are dealt with appropriately in-line with the EWR Risk Management Procedure.

The granularity of the risk assessment may be proportionate to the initial level of risk presented. At a minimum, IT Risk Assessments will always be conducted in alignment with the UK Government Secure by Design Policy (Performing a Security Risk Assessment).

3. Glossary

Please refer to the definitions that are contained within the EWR Glossary.