

\*replace with your company logo

INFORMATION SECURITY

POLICY

# Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the ongoing functioning and good governance of \*COMPANY NAME HERE\*.

Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for \*COMPANY NAME HERE\* to recover.

This information security policy outlines \*COMPANY NAME HERE\* approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of \*COMPANY NAME HERE\* information systems. Support policies provide further details.

\*COMPANY NAME HERE\* is committed to a robust implementation of information security management. It aims to ensure the appropriate confidentially, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which \*COMPANY NAME HERE\* is responsible.

\*COMPANY NAME HERE\* is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties.

# Purpose

The objectives of this policy are to:

* 1. Provide guidelines for establishing suitable levels of information security for all

\*COMPANY NAME HERE\* information systems and to mitigate the risks associated with theft, loss, misuse, damage or abuse of these systems.

* 1. Make certain that users are aware of and comply with all current and relevant UK and EU legislation.
  2. Provide the principles by which a safe and secure information system working environment can be established for all authorised users.
  3. Ensure all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
  4. Protect \*COMPANY NAME HERE\* from liability or damage through the misuse of its IT facilities.
  5. Maintain confidential information at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.

## Scope

This policy is applicable to, and will be communicated to, all \*COMPANY NAME HERE\* users, contractors and third parties who interact with information held by

\*COMPANY NAME HERE\* and the information systems used to store and process it.

This includes but is not limited to: Cloud systems developed or commissioned by

\*COMPANY NAME HERE\*, any systems or data attached to the \*COMPANY NAME HERE\* data or telephone networks, systems managed by \*COMPANY NAME HERE\*, mobile devices used to connect to \*COMPANY NAME HERE\* networks or hold \*COMPANY NAME HERE\* data, data over which \*COMPANY NAME HERE\* holds the intellectual property rights, data over which \*COMPANY NAME HERE\* is the data controller or data processor, electronic communications sent from

\*COMPANY NAME HERE\*.

# Policy

### Information Security Principles

1. Information should be classified in accordance with the \*COMPANY NAME HERE\* information sensitivity policy.
2. Staff with particular responsibilities for information must ensure the classification of that information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.
3. All users covered by the scope of this policy must handle information appropriately and in accordance with its classification level.
4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification. On this basis, access to information will be on the basis of least privilege and need to know.
5. Information will be protected against unauthorised access and processing in accordance with its classification level.
6. Breaches of this policy must be reported.
7. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits and penetration testing.

# Suppliers

All \*COMPANY NAME HERE\* suppliers will abide by \*COMPANY NAME HERE\* information security policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:

When accessing or processing \*COMPANY NAME HERE\* assets, whether on site or remotely

When subcontracting to other suppliers.

# Cloud Providers

Under the GDPR, a breach of personal data can lead to a fine of up to 4% of global turnover. Where \*COMPANY NAME HERE\* uses Cloud services, \*COMPANY NAME HERE\* retains responsibility as the data controller for any data it puts into the service, and can consequently be fined for any data breach, even if this is the fault of the Cloud service provider. \*COMPANY NAME HERE\* will also bear the responsibility for contacting Information Commissioner’s Office concerning the breach, as well as any affected individual. It will also be exposed to any lawsuits for damages as a result of the breach. It is extremely important, as a consequence, that \*COMPANY NAME HERE\* is able to judge the appropriateness of a Cloud service provider’s information security provision.

# Incident Handling

All information security incidents must be reported to \*COMPANY NAME HERE\* Senior Management Team immediately.

Breaches of personal data will be reported to the Information Commissioner’s Office.

# Supporting Policies

Supporting policies have been developed to strengthen and reinforce this policy statement.

All \*COMPANY NAME HERE\* staff and third parties authorised to access \*COMPANY NAME HERE\* network or information systems are required to familiarise themselves with these supporting policies and to adhere to them in the working environment**.**

These policies are:

* \*COMPANY NAME HERE\* Acceptable Encryption Policy
* \*COMPANY NAME HERE\* Acceptable Use Policy
* \*COMPANY NAME HERE\* BYOD Policy
* \*COMPANY NAME HERE\* Password Policy
* \*COMPANY NAME HERE\* Information Sensitivity Policy

# Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Definitions

### Terms and Definitions

\*COMPANY NAME HERE\* Information System Resources

\*COMPANY NAME HERE\* Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Note |
| 1.0 | 21/01/2021 | \*Your Name\* |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |