

Information Security Policy

The confidentiality, integrity, and availability of information, in all its forms, are critical to the on-going functioning of Plastic Surgeon. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for Plastic Surgeon to recover.

This information security policy outlines Plastic Surgeons approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the information systems.

Plastic Surgeon's computer and information systems underpin all Plastic Surgeon's activities and are essential to the delivery of a fine finishing service to its customers. Plastic Surgeon recognises the need for its employees and customers to have access to the information they require in order to carry out their work and recognises the role of information security in enabling this. Security of information must therefore be an integral part of the Plastic Surgeon's management structure in order to maintain continuity of its business.

Purpose

The purpose of this policy is to define requirements for maintaining the integrity of Plastic Surgeons systems. These requirements are designed to minimize the potential exposure to Plastic Surgeon from damages which may result from any unauthorized use, reduced availability, or data breach of Plastic Surgeons resources.

Procedures

The following information security principles provide overarching governance for the security and management of information at Plastic Surgeon.

- (i) Information should be classified according to an appropriate level of confidentiality, integrity and availability. Classifications are covered in more detail within the Data Classification Policy.
- (ii) Staff with particular responsibilities for information must review the classification of all information, handle that information in accordance with its classification level and must abide by any contractual requirements, policies, procedures, or systems for meeting those responsibilities.
- (iii) All users must handle information appropriately and in accordance with its classification level.
- (iv) Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.
 - a. On this basis, access to information will be on the basis of least privilege and need to know.
 - b. Information will be protected against unauthorized access and processing in accordance with its classification level.
- (v) Breaches of this policy must be reported to the IT Director
- (vi) Information security provision and the policies that guide it will be regularly reviewed,

This policy is applicable to and will be communicated to all employees and contractors. It covers, but is not limited to, any systems or data attached to Plastic Surgeon's computer or telephone networks. Coverage includes any communications sent to or from Plastic Surgeon and any data held on systems external to Plastic Surgeon's network.

It is the responsibility of all line managers to implement this policy within their area of responsibility and to ensure that all staff for which they are responsible are 1) made fully aware of the policy; and 2) given appropriate support and resources to comply.

It is the responsibility of each member of staff to adhere to this policy.

Plastic Surgeon is committed to protecting the security of its information and information systems. It is also committed to a policy of education, training, and awareness for information security and to ensuring the continued business of Plastic Surgeon.

It is Plastic Surgeon's policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory, and contractual compliance.


It is Plastic Surgeon's policy to report all information or IT security incidents, or other suspected breaches of this policy. Plastic Surgeon escalates the reporting of security incidents and data breaches that involve personal or customer data to the affected individuals. Records of the number of security breaches and their type will be kept and reported on a regular basis.

Enforcement

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

Distribution

This policy is to be distributed to all staff responsible.

Signed		Date	1 st May 2024
Name Role	Mike Aitken - Managing Director	Review Date	1 st May 2025