1. Overview

Operati strives to ensure the information security of our staff, organisation, customers and the general public across all aspects of its work. Operati adheres to the legal framework under GDPR and best practice guidelines produced by the Information Commissioner's Office (ICO).

2. Physical Security

We ensure compliance to physical security by use of data centres that include:

- CCTV
- E-Card entry controls
- Access to sensitive areas to privilege users only
- BCDR and emergency plans in place to minimise business disruption.
- High standard of security, BCDR and emergency controls with hosting providers.

Internal policies include, but are not limited to:

- Clear Desk and Screen Policy
- Confidential waste disposal procedures

3. Personnel Security

Personnel security includes:

- Vetting processes on recruitment of new employees.
- CRB checks for certain positions or consideration of CVs and following up on references.
- Operati takes out DBS clearance for employees and subcontractors if required.
- Inclusion of confidentiality clauses in all employment contracts.
- GDPR induction and security awareness training as part of the induction process.
- The management systems are password protected with Two Factor Authentication (2FA).

- The server management network is only accessible remotely via Two Factor Authentication (2FA).

4. **Maintenance & Improvement**

   Practices are continually reviewed to ensure their effectiveness and to make improvements where needed.