17. Information Security And Technology

Reviewed By: Melissa Munnich

Review Date: 29th October 2024

The objective of the Company's Information Security Policy (CISP) is to protect the Company's, and its clients' information and information technology from unauthorised access, use, disclosure, disruption, modification or destruction. A copy of the CISP can be found on the Company's intranet.

In implementing the CISP, the Company will seek to ensure the confidentiality, integrity and availability of the Company's and its clients' information by:

- Ensuring that information is accessible only to authorised individuals
- Safeguarding the accuracy and completeness of information by protecting against unauthorised modification
- Ensuring that authorised individuals have access to relevant information when required

All employees have a responsibility to help protect the Company's physical and electronic information assets from threats, whether internal or external, deliberate or accidental. In assisting the Company in implementing the CISP, employees are expected to comply in full with the Company's Information Security Handbook which can be found on the Company's intranet. Any breach of the CISP by an employee through negligence, a deliberate act or misuse may result in disciplinary action up to and including summary dismissal, and may also render the Company and the employee liable to civil or criminal proceedings.

All breaches of information security, actual or suspected, must be reported to the Information Security Officer. Employees who become aware of any violation of the

CISP or any of the rules set out in the Company's Information Security Handbook should report it to the Information Security Officer as a matter of urgency.

In addition, employees working on client sites or who are granted access to clients' information and/or information technology from time to time are strictly required to comply with the clients' rules on information security and information technology as well as the Company's rules. Where there appears to be conflicting rules, employees should consult the Information Security Officer at the earliest opportunity for clarification. If in doubt, employees should follow the stricter rule.

17.1 Monitoring

The Company monitors its compliance with the CISP and specifically employees' adherence to the rules set out in the Company's Information Security Handbook. The Company has the right to monitor and access all aspects of its information technology, including data which is stored on the Company's information technology (whether owned and operated by the

Company or by third parties). Monitoring will take place in accordance with the Company's Monitoring Policy.

17.2 Inappropriate Use

Misuse of the Company's or clients' information and information technology may result in disciplinary action up to and including summary dismissal. Examples of misuse include, but are not limited to, the following:

- Sending, receiving, downloading, displaying or disseminating material that insults, causes offence or harasses others;
- Accessing pornographic, racist or other inappropriate or unlawful materials;
- Engaging in on-line gambling;
- Publishing information which is inappropriate;
- Forwarding electronic chain letters or similar material;
- Downloading or disseminating copyright materials without obtaining the permission of the copyright owner;

- Transmitting or publishing confidential information about the Company or its clients to unauthorised recipients;
- Downloading or playing computer games; and
- Copying, installing or downloading software.

17.3 Passwords

Passwords are essential for securing our organisation's systems and data. Using unique passwords for different accounts reduces the risk of widespread compromise in case one account is breached.

Key Requirements

Password Creation:

- Avoid common words, phrases, or predictable patterns. Use a mix of uppercase, lowercase, numbers, and special characters to ensure a strong password.

Unique Passwords:

- Use a different password for each account or system.
- Do not reuse old passwords or slight variations.

Storage:

- Do not write passwords down or store them in unsecured files.

Additional Security:

- Ensure Multi-Factor Authentication (MFA) is enabled on your accounts.
- Install the Microsoft Authenticator app or another trusted MFA application where required.
- Avoid using personal information as part of your password.

Updating Passwords:

- Change passwords immediately if a compromise is suspected.
- Update passwords immediately if prompted by Microsoft or on other accounts every 3 months

Reporting
If you suspect your password or account is compromised, notify operations immediately and follow their guidance.
Adhering to this policy helps protect our organisation from cyber threats. Ensure all passwords meet these standards.

17.4 Backup and Restoration Testing

Woodhurst conducts backup restoration tests on an annual basis to ensure they operate correctly and meet defined recovery objectives. The results of these tests are reviewed against the live production environment to validate the completeness and accuracy of restored data. Backup data is stored within Microsoft's geo-redundant infrastructure, which ensures separation of data centres by approximately 300 miles to support resilience and regulatory compliance.