Itus Protection Limited
Security and Confidentiality Policy

Our contact details

Name: Itus Protection Limited
Address:167–169
Great Portland Street
London
W1W 5PF

Phone Number: 0330 043 7133
E-mail: Enquires-itusprotection@outlook.com

Security and Confidentiality Policy

1. Introduction

Itus Protection Limited is committed to ensuring the security and confidentiality of all information entrusted to us by our clients, employees, and other stakeholders. This Security and Confidentiality Policy outlines the measures we have implemented to protect sensitive information from unauthorized access, disclosure, alteration, or destruction.

2. Scope

This policy applies to all employees, contractors, and representatives of Itus Protection Limited who have access to sensitive information in the course of their duties, regardless of the format or medium in which the information is stored.

3. Principles

Confidentiality: We will maintain the confidentiality of all sensitive information entrusted to us, including client data, business strategies, and personal information, and will not disclose such information to unauthorized parties without proper authorization.

Security: We will implement appropriate technical, physical, and organizational measures to safeguard sensitive information from unauthorized access, disclosure, alteration, or destruction, ensuring the integrity and availability of the information.

Compliance: We will comply with all applicable laws, regulations, and industry standards relating to data protection, privacy, and confidentiality, as well as contractual obligations with clients and other

third parties.

4. Responsibilities

Management: The management team is responsible for establishing and maintaining a culture of security and confidentiality within the organization, providing leadership and resources to support compliance with this policy.

Employees: All employees have a responsibility to familiarize themselves with this policy, adhere to its principles and guidelines, and report any security incidents or concerns to management or the designated security officer.

Security Officer: The security officer is responsible for overseeing compliance with this policy, conducting risk assessments, implementing security controls, and providing guidance and support to employees on security-related matters.

5. Information Security Measures

Access Controls: We will implement access controls to restrict access to sensitive information to authorized personnel only, using authentication mechanisms such as passwords, encryption, and multi-factor authentication where appropriate.

Data Encryption: We will encrypt sensitive information in transit and at rest to protect it from unauthorized access or interception, using industry-standard encryption algorithms and protocols.

Physical Security: We will secure physical premises, storage facilities, and equipment to prevent unauthorized access, theft, or tampering with sensitive information.

Security Awareness Training: We will provide security awareness training to employees to educate them about security risks, best practices, and their roles and responsibilities in protecting sensitive information.

Incident Response: We will implement procedures for detecting, reporting, and responding to security incidents promptly, minimizing the impact on the confidentiality, integrity, and availability of sensitive information. 6. Confidentiality Obligations

Client Confidentiality: We will respect the confidentiality of client information and will not disclose or use such information for any purpose other than the provision of security services, unless authorized by the client or required by law.

Employee Confidentiality: We will respect the privacy and confidentiality of employee information, including personal data, employment records, and performance evaluations, and will only disclose such information on a need-to-know basis and in accordance with applicable laws and policies.

7. Third-Party Relationships

Vendor Security: We will ensure that third-party vendors and service providers who have access to sensitive information adhere to security and confidentiality requirements, including through contractual agreements and due diligence processes.

Client Agreements: We will enter into written agreements with clients that clearly define the obligations and responsibilities of both parties regarding the protection of sensitive information.

8. Compliance Monitoring and Review
We will monitor compliance with this Security and Confidentiality Policy through regular audits, assessments, and reviews to identify areas for improvement and ensure ongoing effectiveness.

9. Consequences of Non-Compliance

Violations of this Security and Confidentiality Policy may result in disciplinary action, up to and including termination of employment, depending on the severity of the offense. Employees found to have breached security or confidentiality obligations may also be subject to legal action or civil liabilities.

10. Review and Update

This Security and Confidentiality Policy will be reviewed periodically to ensure it remains accurate, relevant, and effective in protecting sensitive information. Changes may be made as necessary to address evolving security threats, regulatory requirements, or business needs.

Conclusion

This Security and Confidentiality Policy reflects our commitment to protecting sensitive information from unauthorized access, disclosure, or misuse. By adhering to the principles and measures outlined in this policy, we can maintain the trust and confidence of our clients, employees, and other stakeholders and safeguard the integrity and confidentiality of the information we handle.
