TECHNICAL POLICY
INFORMATION SECURITY

1. Purpose, Scope and Users

ConstructSecure Inc., (CS), maintains a strong security program that includes policies, procedures, plans, and controls that protect the company's information assets, including but not limited to information technology (IT) systems and sensitive data. The purpose of this policy is to provide a high-level understanding of the principles and practice of ConstructSecure's Information Security Management System (ISMS).

The scope of this policy applies to the entire Information Security Management System, as defined in the CS ISMS Scope document.

Users of this policy are all employees of ConstructSecure, as well as any relevant external parties.

2. Reference Documents

This document was developed as the central information security policy for ConstructSecure. While this policy provides the general approach to information security, it is supplemented by very specific administrative and technical policies, including:

- CS Acceptable Use Policy
- CS Access Control Policy
- CS Change Management and Secure Development/Engineering Policy
- CS Clear Desk and Clear Screen Policy
- CS Data Backup Policy
- CS Document & Information Control Policy
- CS Encryption Policy
- CS Incident Management Policy
- CS Internal & External Audit Policy
- CS Logging and Monitoring Policy
- CS Password Policy
- CS Privacy Policy

In addition to the above policies, the following have also been prepared in accordance with the ISO/IEC 27001:2013 Standard; System & Organization Controls (SOC),

published by the American Institute of Certified Public Accountants (AICPA); the European Union General Data Protection Regulation (GDPR), 2018; the EU-U.S. & Swiss-U.S. Privacy Shield Frameworks and, The California Consumer Privacy Act (CCPA). These documents are also considered reference material to this over-arching Information Security Policy:

- CS ISMS Project Plan
- CS ISMS Statement of Applicability
- CS ISMS Scope Document
- CS ISMS Risk Assessment and Risk Treatment Methodology
- CS ISMS Risk Assessment and Risk Treatment Report

Finally, there are several internal CS manuals that contain information that is relevant to our information security and how we communicate that to employees and clients, including:

- CS Administrative Manual
- CS Customer Support Manual
- CS Disaster Recovery and Business Continuity Manual
- CS Employee Handbook
- CS System Architecture Manual
- CS System Hardening Manual
- CS Vendor Management Manual

3. Information Security Objectives

The three guiding objectives of ConstructSecure's information security are confidentiality, integrity, and availability:

Confidentiality: The goal of confidentiality is to ensure that information is only available to authorized persons or systems. Confidentiality is critical to total data security. In general, the controls that we have in place regarding confidentiality include encryption, virtual private network connections, employee vetting and strict non-disclosure requirements, and many others. Specific controls are fully detailed in the various ISMS supporting documents as listed above in Section 2.

Integrity: The goal of integrity is to ensure that information is only allowed to be changed by authorized persons or systems in an allowed way. This objective includes both data integrity and system integrity. In general, the controls we have in place to

protect the integrity of our data and our system include access control, firewalls, encryption, logging and monitoring, and many others. Specific controls are fully detailed in the various ISMS supporting documents as listed above in Section 2.

Availability: The goal of availability is to ensure that information can be accessed by authorized persons when it is needed. In general, the controls that we have in place regarding availability include authentication, authorization, password control, and many others. Specific controls are fully detailed in the various ISMS supporting documents as listed above in Section 2.

To achieve our guiding objectives, ConstructSecure relies on an overall Information Security Management System that allows for planning, implementing, maintaining, reviewing, and improving information security. While the ideals behind our guiding principles may seem too general to measure, ConstructSecure utilizes the S.M.A.R.T. concept to establish demonstrable ways to determine our success in achieving the confidentiality, integrity, and availability of our system. We have developed a checklist of items that are Specific, Measurable, Achievable, Relevant, and Time-based. This checklist is reviewed twice a year by the Chief Technology Officer and the results are tracked, analyzed, and included as part of the annual ISMS Management Review meeting. The checklist is included as Appendix 1 to this policy.

4. Managing Information Security

This policy, and all referenced documents, outline ConstructSecure's Information Security Management System (ISMS) in order to protect the organization's information assets against all threats, whether internal or external, deliberate or accidental. ConstructSecure relies on the highest standards of practice to meet our security challenges, including those requirements published by the International Organization for Standardization (ISO) as part of ISO/IEC 27001:2003; the American Institute of Certified Public Accountants (AICPA) as part of their System & Organization Controls (SOC); the European Union as part of the General Data Protection Regulation (GDPR); the California Consumer Privacy Act (CCPA); the Payment Card Industry Data Security Standard (PCI DSS); and, best industry practices. This Information Security Policy ensures that the principles of confidentiality, integrity, and availability will be met.

Specific tenets of this Information Security Policy include:

a. Buy-in for the planning and implementation of the ISMS is at the highest level of the organization. Specifically, both the Founder and the Chief Executive Officer have

approved all aspects of the ISMS, including but not limited to this policy and is committed to ensuring that the necessary resources are available to support the ISMS. Both the Founder and the Chief Executive Officer are responsible for staff compliance across the organization.

b. The Information Security Policy ensures that there is clear responsibility for the development and review of information security objectives. Specifically, all technical policies are developed through the joint efforts of the members CS Information Technology Department and are reviewed and published at least annually by the Chief Technology Officer. The Chief Technology Officer is designated as the Information Security Manager as defined by ISO/IEC 27001:2013. All administrative and human resource policies are developed by the Vice President of Compliance and are reviewed at least annually by both the Founder and the Chief Executive Officer.
c. The Information Security Policy ensures that both the Chief Technology Officer and the VP of Compliance formally report to both the Founder and the Chief Executive Officer on the performance of their relevant areas of the ISMS monthly, but due to the small size of the organization and the open working environment conversations about maintaining, improving, and exceeding the requirements of the ISMS are a continual process and are integrated into ConstructSecure's day-to-day business.
d. The Information Security Policy ensures that the ISMS is compliant with relevant legal and regulatory requirements and contractual obligations as detailed in the CS Administrative Manual.
e. The process of selecting appropriate controls and measures to safeguard our information assets is defined in the CS ISMS Risk Assessment and Risk Treatment Methodology and is reviewed continuously by the Chief Technology Officer to ensure that the ISMS is robust and evolves as new security technologies develop.
f. The process of auditing and measuring the effectiveness of our selected controls is conducted as outlined in various ISMS documents, including the CS Internal & External Audit Policy, and with Section 5 below.
g. Business continuity plans will be developed, maintained, and tested as defined in the CS Business Continuity Manual.
h. Training and awareness with this policy, and other referenced ISMS documents, is conducted as part of ConstructSecure's overall employee training program as detailed in the CS Administrative Manual and the CS Employee Handbook. As part of the training, employees are informed about the ISMS, provided with access to reference documents, and must sign off on acknowledgement and agreement with the overall ISMS and, specifically, this policy. In addition, an annual company-wide meeting is held where the ISMS is reviewed to ensure ongoing suitability, adequacy, and effectiveness. Detailed minutes of that annual meeting are prepared and maintained by the VP of Compliance.

i. All actual or suspected security breaches will be reported to the Chief Technology Officer and will be thoroughly investigated as defined in the CS Incident Management Policy. Notification of personal data breaches will be reported to affected users as required by the GDPR, the EU-U.S. & Swiss-U.S. Privacy Shield Frameworks, and as defined in the CS Privacy Policy.

j. All employees, including the Founder, the Chief Executive Officer, and the Chief Technology Officer are committed to continual improvement of the ISMS and work closely with clients to establish the highest quality standards and to ensure that they are partners in our commitment to information security.

5. Measuring the Effectiveness of Information Security Controls

a. Compliance Criteria

When evaluating the effectiveness and adequacy of this particular policy, the following criteria must be considered:

- Number of employees who have a role in the ISMS, but are not familiar with the CS Information Security Policy and know where to access it online;
- Percent of clients and external parties who have been communicated with on the CS Information Security Policy and who have been provided a copy on annual basis (and whenever there is a new version); and,
- Number of reviews of laws and regulations for applicability to ConstructSecure operations in a 6-month period.

b. Compliance Measurement

The specific compliance criteria bulleted above are included as part of an ISMS Comprehensive Compliance Measurement Table that has been prepared by ConstructSecure and is provided in Appendix 1. The Chief Technology Officer and the Vice President of Compliance will verify compliance with our overall Information Security Policy, and all other technical policies, by performing a review, at least annually, using the ISMS Comprehensive Compliance Measurement Table. The results of the annual review will be tracked, analyzed, and included as part of the annual ISMS Management Review meeting.

In addition to the formal annual review, compliance is also measured on a continual basis through various methods, including but not limited to, periodic walk-throughs, business tool reports, and feedback to the policy owner.

c. Exceptions

Any exception to the policy must be approved by the policy owner in advance.

d. Non-Compliance

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

6. Review and Development

The author of this policy is considered the policy owner and is responsible for updating it whenever changes are dictated by the work. In addition, a quarterly review of the Information Security Policy will be conducted by the Chief Technology Officer to ensure that this overarching technical policy remains appropriate considering any relevant changes to the law, organizational policies, and/or contractual obligations.

As specified in the CS Administrative Manual, all changes to an ISMS document must be made using "track changes", making visible only the revisions to the previous version, either showing them in red text or ~~strikeout~~. In addition, for reference, all previous versions of an ISMS document are stored on the personal user drive of the CS Vice President of Compliance. The versioning history is defined in the table below:

Version History	Date	Author	Approver	Classification
Version 5	4/1/21	S. Kirilenko	D. Milinazzo, K. Sardone	Confidential
Version 4	1/21/20	S. Kirilenko	D. Milinazzo, K. Sardone	Confidential
Version 3	5/15/19	S. Kirilenko	D. Milinazzo, K. Sardone	Confidential
Version 2	7/3/18	S. Kirilenko	D. Milinazzo, K. Sardone	Confidential
Version 1	10/24/17	S. Kirilenko	D. Milinazzo, K. Sardone	Confidential
This policy will be reviewed quarterly by the Chief Technology Officer.				

7. Appendices

Appendix 1 – ISMS Comprehensive Compliance Measurement Table.

Appendix 1 – ISMS Comprehensive Compliance Measurement Table

Objective	Measurement	Target	Document Reference	Responsibility
Integrity	Number of employees who have a role in the ISMS, but are not familiar with the CS Information Security Policy and know where to access it online.	0	Information Security Policy	K. Sardone
Integrity	Percent of clients and external parties who have been communicated with on the CS Information Security Policy and who have been provided a copy on an annual basis (or whenever changed).	100%	Information Security Policy	K. Sardone
Confidentiality Integrity Availability	Number of reviews of laws and regulations for applicability to ConstructSecure operations in a 6-month period.	1	CS Administrative Manual	K. Sardone
Confidentiality Integrity	Number of incidents related to unacceptable use of information assets, including instances of asset loss or compromise.	0	Acceptable Use Policy	D. Milinazzo
Confidentiality Integrity	Number of incidents related to inadequate employee training or awareness programs regarding the acceptable use of information assets.	0	Acceptable Use Policy	D. Milinazzo
Confidentiality Integrity	Number of incidents related to unauthorized access into the system.	0	Access Control Policy	D. Milinazzo

Confidentiality Integrity	Number of times unwanted traffic passed the firewall.	0	Access Control Policy	D. Milinazzo
Integrity	Number of incidents arising from failed security controls built into the system.	0	Change Management and Secure Development/Engineering Policy	D. Milinazzo
Confidentiality Integrity	Number of incidents related to unauthorized access to information on desks, printers, photocopiers, fax machines, work stations, etc.	0	CS Clear Desk and Clear Screen Policy	K. Sardone
Integrity Availability	Number of unsuccessful backup tests.	0	CS Data Backup Policy	D. Milinazzo
Confidentiality	Number of incidents related to document errors, including but not limited to, incorrect level of confidentiality and versioning errors.	0	CS Document & Information Control Policy	K. Sardone
Confidentiality	Number of incidents related to unencrypted data.	0	CS Encryption Policy	D. Milinazzo
Integrity	Number of weaknesses or incidents which were not reported to authorized persons.	0	CS Incident Management Policy	D. Milinazzo
Integrity	Number of incidents which were not treated appropriately.	0	CS Incident Management Policy	D. Milinazzo
Integrity	Number of violations of security rules that required that the disciplinary process was invoked.	0	CS Incident Management Policy	D. Milinazzo

Integrity	Incident response volume in a 4-month period.	90% less than the previous quarter	CS Incident Management Policy	D. Milinazzo
Integrity	Average time to detect an incident in a 4-month period.	0	CS Incident Management Policy	D. Milinazzo
Integrity	Average time to correct an incident in a 4-month period.	0	CS Incident Management Policy	D. Milinazzo
Integrity Availability	Cumulative down time of the system in a 4-month period.	0	CS Incident Management Policy	D. Milinazzo
Integrity	Number of incidents that resulted in a change to the Risk Assessment and Risk Treatment table.	0	CS Incident Management Policy	D. Milinazzo, K. Sardone
Integrity	Number of times the Risk Assessment and Risk Treatment table was reviewed in a 12-month period.	2	CS Risk Assessment and Risk Treatment Methodology.	D. Milinazzo, K. Sardone
Integrity	Percent of employees who have a role in disaster recovery and/or business continuity who are familiar with their responsibilities.	100%	CS Disaster Recovery and Business Continuity Manual	K. Sardone
Integrity	Number and type of audits conducted from January to January.	2	CS Internal & External Audit Policy	D. Milinazzo, J. Alamgir
Confidentiality Integrity	Number of penetration tests conducted by a qualified 3rd party in a 12-month period.	1	CS Internal & External Audit Policy	D. Milinazzo

Confidentiality Integrity	Number of audits for compliance with PCI DSS by a qualified 3rd party in a 12-month period.	1	CS Internal & External Audit Policy	D. Milinazzo
Integrity	Number of corrective actions identified during an internal audit.	0	CS Internal & External Audit Policy	D. Milinazzo, J. Alamgir
Integrity	Percent of corrective actions successfully closed out after an internal audit.	100%	CS Internal & External Audit Policy	D. Milinazzo
Confidentiality Integrity	Number of incidents related to misuse of passwords by unauthorized persons	0	CS Password Policy	D. Milinazzo
Confidentiality Integrity	Number of incidents related to inadequate handling of passwords.	0	CS Password Policy	D. Milinazzo
Integrity	Percent of employees who completed ISMS training in a 12-month period.	100%	CS Employee Handbook	K. Sardone
Integrity	Percent of employees who know where to access the ISMS supporting documentation?	100%	CS Employee Handbook	K. Sardone