MINIMUM INFORMATION SECURITY REQUIREMENTS FOR SUPPLIERS

CHQ-IS-POL-021

Approved by	ISMS Steering Committee

Rev.	Date	Description of Change
0	05/23/2025	First issue
1	08/20/2026	Name and Logo Change

`

Contents

`

1.0 Purpose & Scope

To uphold the Organization's commitment to ISO 27001 ISMS requirements, this document has been developed to outline information security expectations for suppliers and their practices when managing the Organization's data.

All suppliers providing services to CSP Innovations, Inc. (further referred to as “Organization”) must comply with, as a minimum, the information security requirements in this document.

These requirements are in addition to all other contractual obligations between the Organization and the supplier.

The term “Organization’s Information” used in this document includes information owned by CSP Innovations, Inc. and handled by the supplier in provision of their services. This includes any client or other third-party owned information handled by the supplier.

This document is intended to safeguard the confidentiality, integrity, and availability of sensitive information while ensuring that authorized suppliers can efficiently carry out their responsibilities. By implementing the Minimum Information Security Requirements for Suppliers, we aim to secure critical data, minimize risks, adhere to regulatory standards, and strengthen trust among our stakeholders.

This document is designed to adhere to industry best practices, comply with regulatory requirements, and support the Organization's risk management objectives.

Compliance with this document is required from any Supplier handling the Organization’s information. The Organization recognizes that there might be instances where certain requirements could not be met. Deviations must be reported to the Organization’s designated point of contact and will be evaluated on a case-by-case basis.

2.0 Requirements

2.1 Confidentiality

Supplier must maintain confidentiality of the Organization’s Information.

Supplier must not share the Organization’s information with third parties without Organization’s approval.

2.2 Secure Methods

Supplier must use secure methods of storage, processing and transmission of Organization’s Information (e.g., passwords, encrypted email, secure file transfer).

2.3 Access Management

Suppliers shall implement a process for control of access to the systems and applications where Organization’s data is being processed or stored.

Access rights shall be revoked for users who no longer need system access.

2.4 Information Security Incidents

Suppliers must inform the Organization about Information Security Incidents that have compromised or may potentially compromise the Organization's data, such as data breaches, unauthorized access, or suspicious activity.

Supplier shall support any investigation (e.g. by the Organization, law enforcement, or regulatory authorities) that involves Organization’s Information.

`

2.5 Compliance

Suppliers are required to comply with applicable Information Security and data protection laws.

Any and all requirements stated in the Contract and other Agreements (e.g. NDA) between the Organization and the Supplier must be followed.

2.6 Subcontractor Management

Supplier Agreements with third parties handling the Organization's Information must incorporate appropriate information security, confidentiality, and data protection provisions.

Supplier must restrict third party access to the Organization’s Information and grant such access to authorized third parties only.

2.7 Service Termination

Supplier must comply with a process for service termination or conclusion. Confidentiality and non-disclosure obligations regarding the Organization's Information shall continue beyond the termination or conclusion of the Agreement.

Supplier must ensure that the Organization’s Information is securely destroyed when no longer needed for the purposes authorized by the Organization or at the expiration or termination of the Agreement.

2.8 Acknowledgement

By proceeding, you acknowledge and agree to comply with the requirements stated above. Failure to comply may result in corrective actions or restrictions in access. Thank you for your cooperation in maintaining a secure environment.