	SIKRI TECHNICAL & VOCATIONAL COLLEGE FOR THE BLIND AND DEAF	
	INTEGRATED MANAGEMENT SYSTEM BASED ON ISO 9001 AND ISO/IEC 27001	
	DOCUMENTATION MANUAL	
	APPROVED BY: Principal	ISSUED BY: Management Representative

POLICY NUMBER 16: SUPPLIER SECURITY

1.0 PURPOSE

The purpose of this document is to define the rules for relationships with suppliers and partners, including the providers of cloud services.

2.0 SCOPE

This document is applied to all suppliers and partners who have the ability to influence confidentiality, integrity and availability of STVCBD's sensitive information.

3.0 USERS

Users of this document are top management and persons responsible for suppliers and partners in STVCBD

4.0 REFERENCE DOCUMENTS

- a) ISO/IEC 27001:2013 standard, clauses A.5.7, A.5.11, A.5.19, A.5.20, A.5.21, A.5.22, A.5.23, A.6.1, A.6.2, A.6.3 and A.8.30
- b) Risk Assessment and Risk Treatment Methodology
- c) Risk Assessment and Risk Treatment Report
- d) Access Control Policy
- e) Confidentiality Statement

5.0 POLICY PROVISIONS

5.1 Relationship with suppliers and partners - Identifying the risks

5.1.1 Security risks related to suppliers and partners, including the providers of cloud services, are identified during the risk assessment process, as defined in the Risk Assessment and Risk Treatment Methodology.


5.1.2 During risk assessment, special care shall be taken to identify risks related to information and communication technology, as well as risks related to product supply chain.

5.1.3 The Procurement officer in liaison with user departments shall decide whether it is necessary to additionally assess risks related to individual suppliers or partners.


5.2 Screening

The Procurement officer shall decide whether it is necessary to perform background verification checks for individual suppliers and partners, and if yes – which methods shall be used. E.g. experience of their other clients, credit history, onsite audit, etc.

5.3 Contracts

	SIKRI TECHNICAL & VOCATIONAL COLLEGE FOR THE BLIND AND DEAF	
	INTEGRATED MANAGEMENT SYSTEM BASED ON ISO 9001 AND ISO/IEC 27001	
	DOCUMENTATION MANUAL	
	APPROVED BY: Principal	ISSUED BY: Management Representative

- 5.3.1 User department shall be responsible for deciding which security clauses will be included in the contract with a supplier or partner. Such decision shall be based on the results of risk assessment and treatment.
- 5.3.2 The following clauses are mandatory in the agreements with suppliers:
- a) Keeping the confidentiality of the information
 - b) Return of assets after the termination of the agreement
How the information about threats is communicated between the supplier and the
 - d) Ensuring a reliable delivery of the products and services, which is particularly important with cloud service providers
- 5.3.3 The Procurement officer in liaison with user department shall decide whether the individual employees of the supplier/partner will have to sign the Confidentiality Statements when working for STVCBD
- 5.3.4 User department shall decide who will be the contract owner for each contract – i.e. who will be responsible for a particular supplier or partner.
- 5.4 Training and awareness
- 5.4.1 Contract owner shall decide which employees of suppliers and partners need security awareness and training.
- 5.4.2 The HRO shall be responsible for providing all the training and raising of awareness of those employees.
- 5.5 Monitoring and review
- 5.5.1 Contract owner shall regularly check and monitor the level of service and fulfillment of security clauses by suppliers or partners, reports and records created by the supplier/partner, as well as audit the supplier or partner at least once a year.
- 5.5.2 All the security incidents related to the partner's/supplier's job shall be forwarded immediately to Management Representative
- 5.6 Changes or termination of supplier services
- 5.6.1 Contract owner proposes changes or termination of the contract, and Principal makes the final decision. If necessary, contract owner will perform a new risk assessment before the changes are accepted.
- 5.7 Removal of access rights / return of assets

	SIKRI TECHNICAL & VOCATIONAL COLLEGE FOR THE BLIND AND DEAF	
	INTEGRATED MANAGEMENT SYSTEM BASED ON ISO 9001 AND ISO/IEC 27001	
	DOCUMENTATION MANUAL	
	APPROVED BY: Principal	ISSUED BY: Management Representative

- 5.7.1 When the contract is changed or terminated, the access rights for employees of partners/suppliers shall be removed according to the Access Control Policy.
- 5.7.2 Further, when the contract is changed or terminated, the contract owner shall make sure all the equipment, software or information in electronic or paper form is returned.