Partners Cybersecurity Controls Guideline

Table of Contents

1. Objective 5
2. Cybersecurity Controls' Requirement 5
3. General Requirements 5

1. Objective

The objective of Security Pass Program is to ensure all partners adherence to the cybersecurity requirements in stc Partners Cybersecurity Standard by obtaining Security Pass Certification from an Authorized Audit Firm. This manual will provide stc partners with the required guidance to fulfill the cybersecurity controls' requirements for each control. This will ensure that supported, required and comprehensive evidences are provided part of the partner compliance package that will be submitted to authorized audit firm.

2. Cybersecurity Controls' Requirement

The cybersecurity controls guidance document must be used as a reference to ensure unified expectations for the evidences to be provided for each cybersecurity control. The guideline must be utilized for remote assessments where partners must provide a comprehensive assessment package in accordance to all the controls' requirements stated in this document. Moreover, this guideline can be used for on-site assessments where audit firms can verify the evidences against each control's requirements. In case of inapplicability, partner must fill the inapplicability form with required justifications for each inapplicable control.

3. General Requirements

Control #	Control Statement	Controls' Requirements
SP-1	Partner must have policies and processes to classify information in terms of its value, criticality, confidentiality, and sensitivity.	- Provide evidence of the partner data classification policy Provide evidence of the partner Data Classification program that cover all key resources (e.g., hardware, devices, data, software) are classified based on risk
SP-2	The Partner must be staffed by a full-time employee whose primary responsibility is Cybersecurity. Responsibilities of that personnel must include maintaining the security of information systems and ensuring compliance with existing policies.	- Provide a copy of the organizational chart. - Provide evidence of job descriptions, agreements, RACI charts, service level agreements (SLAs) and/or contracts to determine if they include cybersecurity roles and responsibilities.
SP-3	The Partner must establish, maintain, and communicate Cybersecurity Policies to all employees. Cybersecurity Policies must be reviewed on a yearly basis. Updates must be communicated to all employees in keeping with Partner Company Policies.	- Provide evidence of the partner Cybersecurity Policies and Standards. - Provide evidence of communicating Cybersecurity Policies to employees. - Provide different policy updates versions

SP-4	The Partner must establish, maintain, and communicate a Cybersecurity Acceptable Use Policy (AUP) governing the use of Partner Assets. Cybersecurity AUP must be reviewed on a yearly basis. Updates must be communicated to all employees in keeping with Partner Company Policies.	- Provide a copy of approved (AUP) - Provide sample of communication regarding sharing (AUP) to employees - Provide different versions of approved and communicated AUP, that shows different releases and updates
SP-5	Security Waiver process must be in place for approving any deviation from information security policies, standards, procedures and/or practices. Granted waivers must be retained and reviewed annually.	- Provide evidence for Waiver process. - Provide evidence for annual review.
SP-6	The Partner must conduct annual Penetration Testing on their IT infrastructure.	- Provide evidence of Penetration testing reports conducted and analyzed on IT infrastructure considering all critical, internal, and external systems. - Provide evidence of a policy tackling penetration test schedule, scope and requirements exist and communicated to stakeholders - Provide evidence of remediation and action plan related to penetration test results.
SP-7	The Partner must have a Risk Management process in place to identify, assess and remediate Risks to information systems.	- Provide evidence of the framework or process used for risk management. Consider the following. - Provide evidence of the organization's risk management plan showing the organization's response to risk levels - Provide evidence of risk register - Provide evidence of risk management plan that is designed to accept or reduce risk level in accordance with the organization's risk appetite/ tolerance.
SP-8	Users accessing information systems must be issued unique user logins and passwords. Generic accounts must not be allowed.	- Provide evidence of access management policy that shows the requirement of using unique accounts. - Test sample of servers/ systems to determine if unique account is used for on-site assessment.

SP-9	Password protection measures must be enforced by the Partner. The following are recommended measures: - Minimum length: 8 alphanumeric characters and special characters. - History: last 12 passwords - Maximum age: 90 days for login authentication - Account lockout threshold: 10 invalid login attempts. - Screen saver settings: automatically locked within 15 minutes of inactivity.	- Provide technical check evidence to confirm the compliance of the control requirements. - Provide evidence of the password configuration on Active directory to ensure that default settings are not used. If active directory does not exist, provide evidence from the local password policy on sample systems. - Provide a copy of password policy that should comply with the control requirements and technical check findings.
SP-10	Partner must not write down, electronically store, or disclose any password or authentication code that is used to access Assets or Critical Facilities.	- Provide a copy of password disclosure policy - Provide a copy of actions taken in case password disclosure happened part of the consequence management
SP-11	Permanent security badges must be issued to Partner employees. Personnel must wear picture identification badges always.	- Provide evidence of a policy that state the requirement of wearing security badges - Provide a sample of partner security badges.
SP-12	Partner must define a process for visitor management. The process should include maintaining and regularly reviewing visitor logs and issuing temporary visitor badges. The visitor log should capture information such as: - Visitor National / Iqama ID - Visit Purpose - Check in/check out date and time	- Provide evidence of the partner visitor management policy - Provide evidence of visitor logs, including the following: - Visitor National / Iqama ID - Visit Purpose - Check in/check out date and time
SP-13	All privileged accounts such as "Administrator" and "root" must be restricted to a limited number of authorized users. The accounts' activity must be logged and monitored on a regular basis.	- Provide evidence of a policy that shows the procedure of obtaining and revoking the admin privileges based on the job requirements/ function - Provide evidence of the partner process to identify privileged users. - Provide evidence of privileged

		accounts reviewed regularly.
SP-14	The Partner must dedicate an access restricted working area for personnel with access to stc network.	- Provide evidence of dedicated working area is allocated for stc projects and workstations. - Provide evidence of physical security control implementation on stc working area.
SP-15	The Partner must logically (e.g. partitioning a physical drive) and/or physically segregate data related to stc from the data of any other clients or customers.	- Provide evidence of logical segregation on physical drives use to store stc data. - Provide evidence of physical segregation including dedicated data room/ files for stc data. - Provide evidence of Partner Policy of treating partner data including stc.
SP-16	The server and workstation subnets must be segmented and access between them is restricted and monitored on a regular basis.	- Provide evidence of server and workstation subnets are segmented. - Provide evidence of a range of subnets assigned on different assets - Provide evidence of monitoring the segmentation.
SP-17	Servers accessible from the Internet must be placed in a DMZ (i.e. perimeter network) with restricted access to internal subnets.	- Provide evidence of high-value/critical systems are separated from high-risk systems (e.g., VLAN, DMZ, hard backups, air-gapping) where possible. - Provide evidence of network diagrams and data flow diagrams. - Provide evidence of monitoring the traffic travels between different DMZ zone and internal subnets.
SP-18	Remote connections to information systems at the Third Parties location must be authorized, monitored and have two-factor authentication.	- Provide evidence of policies and procedures related to remote users' access capabilities are formalized. Consider that remote users (e.g., employees, Partner, Partners) with access to critical systems are approved and documented and remote - connections are logged and monitored.

SP-19	Wireless networks accessing information systems at the Third Parties location must use strong encryption for authentication and transmission, such as WPA2 or WPA2 Enterprise.	- Provide evidence of access point configuration. Provide evidence of Wireless baseline details.
SP-20	Partner must not use traffic anonymizers, proxies or sites redirectors when accessing stc services.	- Provide an official letter for not using traffic anonymizers, proxies or sites redirectors.
SP-21	Partner must inform stc when employees provided with stc user credentials no longer need their access, or are transferred, re-assigned, retired, resigned or no longer associated with the Partner.	- Provide the partner policy/contract in term of dealing with stc credentials. - Provide a sample of communication (Email) to stc to revoke invalid accounts. Provide evidence for revoked accounts that are invalid accounts for people who are retired, resigned, or no longer associated with the Partner.
SP-22	The Partner must require all information systems users to take a yearly mandatory Cybersecurity training that addresses acceptable use and good computing practices. Training must address the following topics: 1. Internet and social media 2. Acceptable Use 3. Phishing emails 4. Sharing credentials (i.e. username and password) 5. Data Protection	- Provide acceptable use policy and/or training materials to ensure content is adequate. - Provide user training reports and/or documentation to ensure users are trained in accordance with applicable policy, guidance, and/or requirement (e.g., annual cybersecurity training of all employees). - Provide evidences of updating the training materials based on changes in cyber threat environment.
SP-23	The Partner must inform personnel, in keeping with Partner Company Policy, that using personal email to share and transmit stc data is strictly prohibited.	- Provide Partner Company Policy and contract of using personal email. - Provide the Partner policy / contract ensure partners are complying with cybersecurity responsibilities defined in contracts and agreements. -Provide related emails communicated to partner's employees to ensure the compliance of this control. - Provide relevant counter measure that partner has taken to comply with the control requirements.

SP-24	The Partner must inform personnel, in keeping with Partner Company Policy, that disclosing stc policies, procedures and standards or any type of data with unauthorized entities or on the Internet is strictly prohibited.	- Provide Partner policy including contracts and agreements that highlight the prohibited disclosure of stc related data. -Provide related emails communicated to partner's employees to ensure the compliance of this control - Provide relevant counter measure that partner has - taken in case of disclosing stc Data
SP-25	All Partner devices such as systems, workstations and laptops must be password protected.	- Provide evidence of related assets management policy that define Technology assets' protection. - -Provide evidence of related policy for all partner systems to be password protected.
SP-26	The "Remember Passwords" feature must be disabled in web browsers.	- Provide evidence of the partner baseline configuration for all web Browsers. - Provide evidence of the group policy that will disable the browser's native password manager. - Provide evidence of all web browsers settings for password disablement
SP-27	Backup media must be secured so as to block/inhibit unauthorized physical access.	- Provide evidence of backup media physical security controls implemented. - Provide evidence of backup media related policy and configuration.
SP-28	Partner workstations, laptops and servers must be regularly updated with operating system (OS), software and applets patches (i.e. Adobe, Java etc.)	- Provide evidence of patch management policy and procedures - Provide evidence of on sample of workstations to ensure that OS and software are up to date - Provide evidence of scheduling and technology used for patch and updates deployment.
SP-29	The Partner must protect every workstation, laptop and server with anti-virus (AV) software. Updates must be applied daily, and full system scans must be performed weekly.	- Provide evidence of the anti-virus installed on endpoint devices - Provide evidence of configuration console of the installed anti-virus software to determine the last updates and full system scan that were performed - Provide evidence of the history of updates

SP-30	for remote access to stc, The partner must implement/utilize encryption technologies to protect the confidentiality and integrity of transmitted information (e.g. SSH, FTPS, HTTPS, IPSEC).	- Provide evidence of web security appliance to ensure that encryption technology are used and enabled when data is transmitted across publicly accessible networks. - Provide evidence of adequate policies are in place regarding transmission of data, especially the one transmitted via email.
SP-31	The partner must employ encryption mechanisms, using at least AES encryption algorithm, and 256 bit key, on all devices or storage media hosting sensitive data per the partner's assets tiering policy.	- Provide evidence of encryption mechanisms applied on all devices, including disk drives by checking BitLocker Drive encryption. - Provide evidence of a policy ensuring mobile devices (e.g., laptops, tablets, and removable media) that are used to store confidential data are encrypted.
SP-32	The Partner must employ a device control mechanism on Assets that are used to receive, store, process or transmit stc data such as disabling USB drivers.	- Provide evidence of assets used to perform/conduct stc business with removable media restrictions to ensure restrictions are working as expected and comply with the organization's policy. - Provide evidence of the removable media policy, which may include: o Encryption of removable media - Restricted access to removable media (e.g., USB restrictions)
SP-33	Access to the Internet must be restricted by Content-filtering technologies to restrict access to non-business-related websites, web-based email and cloud Storage services.	- Provide evidence of the technology used for content filtering - Provide evidence of no related business site like malicious websites being blocked. - Provide evidence of appropriate configuration for accessing web-based email, cloud Storage services.
SP-34	Partner must implement Sender Policy Framework (SPF) technology on the mail server.	- Provide evidence of SPF implementation on the third-party mail server.
SP-35	Documents containing stc Confidential Information, or higher classification, must be encrypted and password- protected at all times.	- Provide evidence of policy where documents must only be shared with limited individuals who are part of the work specified in the Contract. - Provide evidence of documents with

		Passwords to unlock these documents: o Must never be stored. o Must never be shared in the same communication method (e.g. email) as the documents. o Must be communicated to the recipient(s) over the phone, in person or via SMS text message. o Must be in line with the password protection measures stated in Control Number "SC-2" in this Standard in agreement with a stc eligible recipient of the document. - -Provide evidence for hardcopy documents being stored securely in dedicated and locked cabinet with access limited to authorized personnel.
SP-36	Remote wipe solution must be installed on any Assets used to receive, store and/or produce Confidential Information, or higher classification, for stc.	- Provide evidence of ability to wipe data remotely on mobile devices when data are missing or stolen is enabled. - Provide evidence of policy related to remote access and remote wipe solution used
SP-37	Partner must create and manage baseline configurations to harden information systems. The hardening process must address configurations such as resetting default usernames/passwords and not allowing non-business-related software.	- Provide evidence of the baseline configurations for systems (e.g., servers, desktops, routers). - Provide evidence of samples against the partner's baseline configurations to ensure standards are followed and enforced, for the following: - Resetting default usernames/passwords - Disabling unneeded software - Disabling unneeded services - Removing administrative access of users on workstations.
SP-38	The Partner must establish and follow regular procedures for backup of information and software. If backup is stored at an off-site location, it must be encrypted using at least AES encryption algorithm, and 256 bit key.	- Provide evidence of partner backup policy, process and procedures. - Provide evidence of the backup tapes are encrypted for off-site location.

SP-39	The Partner must employ a sanitization process before any Assets are loaned, donated, destroyed, transferred, or surplused. The process must be aligned to industry best practices.	- Provide evidence of media sanitization (data destruction) policies. - Provide evidence of sanitization techniques and procedures are commensurate with the security category or classification of the information or asset and in accordance with organizational standards and policies. - Provide proof (e.g., destruction certificates) that media sanitization is occurring according to policy.
SP-40	Partner must have a Disaster Recovery Plan (DR Plan) which is documented, maintained and communicated to appropriate parties. The DR Plan should address the recovery of Assets and communications following a major disruption to business operations.	- Provide evidence of Disaster Recovery plans addressing the control requirements. - Provide evidence of samples of communicating DR to responsible parties and stakeholders.
SP-41	Partner must have a comprehensive Business Continuity (BC) plan which is documented, maintained, and communicated to appropriate parties. The BC plan should address the occurrence of the following scenarios: a) Equipment failure. b) Disruption of power supply or communication. c) Application failure or corruption of database. d) Human error, sabotage or strike. e) Malicious Software attack. f) Hacking or other Internet attacks. g) Social unrest or terrorist attacks. h) Environmental disasters. i) Emergency contact information for personnel.	- Provide evidence of business continuity plans to determine if the partner has documented how it will respond to a cyber-incident. - Provide evidence of the BC plan, which includes all the related subjects/ topics of the control requirements.

SP-42	Partner must ensure that owners of the Business Continuity (BC) plan are identified, and that the BC plan is reviewed and updated annually.	- Provide evidence of the plan to ensure that Business Continuity (BC) plan owners are identified. - Provide evidence of different plans releases to - determine how frequently they are updated and approved.
SP-43	Partner must conduct Business Continuity drills at least annually.	- Provide evidence of business continuity tests / drills are performed according to the policy as required by - the control.
SP-44	Partner must have formal procedures for on-boarding and off-boarding employees. On- boarding procedures must include background checks (e.g. Verification of work histories). Off-boarding procedures must include the removal of all access to Assets.	- Provide evidence of hiring procedures to determine whether background checks/screenings are performed for all employees. - Provide HR screening policy.
SP-45	The Partner must undergo annual audits to ensure the conformity of their cybersecurity practices against the requirements of this standard. Findings relating to Partner conformity to this standard must be remediated within 90 days.	- Provide evidence of the annual audit.
SP-46	The Partner must retain all audit logs from information systems storing, processing, or transmitting stc data for one (1) year.	- Provide evidence of audit logs (e.g., security, activity) are maintained and reviewed in a timely manner. - Provide evidence of Log files are sized such that logs are not deleted prior to review and/or being backed up. - Provide evidence of the partner policy of logs handling - Provide evidence of Audit logs and log management & analysis tools that are protected from unauthorized access, modification, and deletion. - Provide evidence of Audit records contain appropriate content (e.g., type of event, when the event occurred, where the event occurred, source of the event, and outcome of the event, identity of any - individuals or subjects associated with the

		event).
SP-47	All systems (routers, switches, servers, and firewalls) must be housed in a communication room and locked rack(s). The access to the communication room must be contingent on security requirements such as access card readers or biometric devices.	- Provide evidence of Physical security controls are used to prevent unauthorized access to telecommunication systems. - Provide evidence of access is restricted to authorized people.
SP-48	User access to the operating system, applications and database must be reviewed on a semi-annual basis to determine if accessing personnel still require such access.	- Provide evidence of access management policy. - Provide evidence of user access profiles are consistent with their job functions (based on least privilege). - Provide evidence of role-based access controls are implemented (e.g., roles vs. users are assigned access rights). - Provide evidence that ensure excessive permission - are not granted.
SP-49	Firewalls must be configured and enabled on endpoint devices.	- Provide evidence of the firewall setting for all partner endpoint devices including related policies for enabling firewalls. - Provide evidence of the firewall being enabled on domain, public and private firewall settings on sample of partner endpoint devices.
SP-50	Firewalls must be implemented at the network perimeter and only required services must be allowed. Vulnerable services or insecure protocols should be blocked.	- Provide evidence of firewall settings ensure that rules are configured to allow only required services and unneeded protocols and vulnerable services are closed and blocked. - Provide evidence of network diagram for firewalls placement.
SP-51	Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) must be implemented at the network perimeter.	- Provide evidence of IPS/IDS configurations and enablement.
SP-52	Signatures of firewalls and IDS and IPS must be up to date.	- -Provide evidence of firewalls, IDS and IPS signature up-to-date.

SP-53	Partner must have an incident response procedure	- Provide evidence of the incident response plan to determine if there is a process to formally analyze and classify incidents based on their potential impact. - Provide incident response plan to determine if it is designed to prioritize incidents, enabling a rapid - response for significant incidents or vulnerabilities.
SP-54	The Partner must periodically aggregate and correlate data from multiple systems such as Firewalls, IDS/IPS, and anti-virus for event monitoring and analysis	- Provide evidence of listing of event aggregation and monitoring systems in use at the organization (e.g., SIEMs, event log correlation systems). - Provide evidence of list of sources that provide data to each event aggregation and monitoring system (e.g., - firewalls, routers, servers).
SP-55	Multiple physical security measures must be implemented to prevent unauthorized access to facilities. Entrances and exits must be secured with authentication card key, door locks and monitored by video cameras.	- Provide evidence that physical access to key assets (e.g., server rooms, network closets, zones) are physically restricted: • Locked doors • Surveillance • Fences or walls • Logs • Visitor escorts - Provide evidence of policies and procedures allow only authorized personnel access to sensitive areas. - Provide evidence of termination /off-boarding procedures to ensure physical access is removed once - an employee leaves.
SP-56	Non-authorized devices (such as personal devices and mobile phones) must not be used to store, process or access Assets.	- Provide evidence of policies of using personal assets.
SP-57	Monthly Vulnerability scans must be conducted to evaluate configuration, Patches and services for known Vulnerabilities.	- Provide evidence of the partner vulnerability management plan and ensure it includes the following: - Frequency of vulnerability scanning - Method for measuring the impact of vulnerabilities identified (e.g., Common Vulnerability Scoring System

		- Incorporation of vulnerabilities identified in other security control assessments (e.g., external audits, penetration tests) - Procedures for developing remediation of identified vulnerabilities - Provide evidence of samples of vulnerability scan reports. - Provide Vulnerability scanning policy.
SP-58	Physical access to the facility where information systems reside must be restricted and monitored.	- Provide evidence of an inventory of critical facilities (e.g., data centers, network closets, operations centers, critical control centers). - Provide evidence of physical security monitoring controls are implemented and appropriate to detect potential cybersecurity events (e.g., sign in/out logs, motion detectors, security cameras, security lighting, security guards, door/window locks, automatic system lock when idle, restricted physical access to servers, workstations, network devices, network ports).
SP-59	Information systems must log auditable events as stated in Appendix C.	- Provide a list of the monitoring controls implemented by the partner at the application/user account level (e.g., account management, user access roles, and user activity monitoring, file and database access). - Provide evidence of monitoring reports includes detection and alerting of cybersecurity events (e.g., unauthorized account access, unauthorized file/system access, access out of hours, access to sensitive data, unusual access, unauthorized physical access, privilege escalation attacks). - Consider Appendix C on Partner Standard.
SP-60	Incident management policy and procedures must be documented, maintained, and communicated to management and appropriate team members.	- Provide evidence of incident management policy and procedures to determine if reporting structure and communication channels are clearly defined. - Provide evidence that employees are trained to report suspected security incidents. - Provide copies of reports from recent incidents to validate reporting is consistent and follows the plan.

SP-61	Any damage or unauthorized access to Assets that are used to host stc data must be reported to stc within one (1) – two (2) hour(s) of discovery of the Incident.	- Provide evidence of the partner cybersecurity Incident management policies and procedures that conform with the requirements of this control.
SP-62	The Partner must have an Incident Response capability that includes preparation, detection and analysis, containment, eradication, recovery, documentation and reservation of evidence, communication protocols and lessons learned.	- Provide evidence of the incident response plan to determine if appropriate steps are taken consider the following: • Obtain evidence of event notifications (e.g., detection alerts, reports) from different systems. • Determine who receives alerts or reports from detection systems and what actions are taken once reports are received. • Review the incident response plan to determine if actions taken follow the plan. • Steps to contain and control the incident to prevent further harm • Procedures to notify potentially impacted Partners • Strategies to control different types of incidents (e.g., distributed denial-of-service [DDoS], malware, etc.) • Steps to mitigate the incident to prevent further harm • Review any documented incidents to determine whether mitigation efforts were implemented and effective - Review the organization's incident handling reports and incident testing documentation for action items and lessons learned.
SP-63	The Partner must track, classify, and document all Cybersecurity Incidents.	- Provide evidence of the incident response plan to determine if there is a process to formally analyze and classify incidents based on their potential impact. - Provide incident response plan to determine if it is designed to prioritize incidents, enabling a rapid response for significant incidents or vulnerabilities.

SP-64	The Partner must resolve or mitigate the identified security Vulnerabilities on a system, computer, network, or other computer equipment within the following timeframes: - Critical Risk: immediate correction up to three (3) calendar days of critical vendor patch release, notification from stc, or discovered security breach whichever is earlier. - High Risk: within seven (7) calendar days of vendor patch release, or discovered security breach whichever is earlier. - Medium Risk: within one (1) month of occurrence. - Low Risk: within three (3) months of occurrence.	- Provide evidence of the organization's schedule for performing internal and external vulnerability scans and the results of the most recent internal and external vulnerability scans. - Review the schedule and results for the following: • Frequency • Successful completion • Documented resolution or mitigation of identified vulnerabilities • Scope of testing includes all critical systems - Provide evidence of vulnerability scan results were reported to individuals or teams with appropriate authority to ensure resolution. - Provide Vulnerability scanning policy.