D-ST-100002

stc Partners Cybersecurity Standard

Version 1.0 (Date effective: 9/2022, /1443H)

Release Date: 8/2022

Document No. ST- 100002

View Level (Public)

Caution:

- This document is electronically controlled, and only hard copies, identical in version no. 1 to those published in the P&P e-Library, are considered.
- This document should be updated before 60 months of its effective date.

1 Table of Content

2 PURPOSE

The purpose of the **stc** Partners Cybersecurity Standard is to ensure the protection of assets against the Cybersecurity risks related to all third parties including outsourcing and managed services as per ***stc*** cybersecurity policies, standards, and related laws and regulations applicable within ***stc* environment**.

The standard is also intended to provide guidance for maintaining a secure relationship with ***stc*** referred to in the standard as **stc Partners**.

3 SCOPE

This standard is applicable to all business functions and projects of ***stc*** that are acquiring external services, with one or more of the activities and categories set by stc procurement team.

All Partner, consultants, third party staff, apprentices and participants accessing or managing ***stc*** information assets and resources must comply with **stc** Partners Cybersecurity Standard.

All cybersecurity controls specified in this Standard must be implemented on:

- All Partner information systems and/or Assets used to access **stc**' s network.
- All Partner's Assets hosting, receiving, storing, processing, or transmitting **stc** data.
- These Assets must be secured and stored in keeping with this Standard and must be made available to authorized users only on a need-to-know basis.

4 DOCUMENT MANAGEMENT

This document is owned and maintained by the Cybersecurity GRC General Department.

5 Partners Pre-qualification

5.1 All Partners shall go through technical prequalification and certification track (Security Pass Program) to meet *stc* requirements.

5.2 Partners must ensure adherence with cybersecurity controls in this Standard of any further granted access and/or privileges by stc for the Partner to execute the work specified in the Contract.

5.3 The Partner will be granted a grace period of ninety (90) days from the date of awarding the contract to fully implement this standard.

5.4 In the event of a Cybersecurity Incident, the Partner must, besides its continuous efforts to resolve and mitigate the Cybersecurity Incident, follow the Cybersecurity Incident Response instructions specified in Appendix A.

5.5 The Partner either current or new, shall sign the data processing agreement and the data protection agreement attached in Appendix G.

6 Partners Cybersecurity Governance

6.1 All security requirements shall be addressed before granting Partner access to stc information and resources.

6.2 All stc employees of temporary employment agencies, Partners, business partners, and contractor personnel and functional units regardless of geographic location, shall not disclose to anyone outside stc any information related to stc customers.

6.3 Partner shall ensure communication procedures in case of Cybersecurity incidents are included.

6.4 Partner 's dispatched team shall sign an NDA with stc to preserve confidentiality of stc information.

6.5 Partner shall ensure that policies and procedures are in place and followed to prohibit the unauthorized disclosure of knowledge, information, architecture, or configuration relevant to stc 's system.

6.6 Partner should confirm that any proposals or contracts signed with stc are in line with the requirements stated in this document.

6.7 Partner shall provide a Security baseline (MBSS) for all system components.

6.8 stc developed software, documentation, and all other types of internal information shall not be sold or otherwise transferred to any non- stc group party for any purposes other than those expressly authorized by management.

6.9 To gain access to the stc internal network, every Partner shall use a secure system provided by stc or approved by stc.

6.10 stc shall audit all connected systems without warning and in case of non-compliance, stc shall immediately terminate network connections with all Partner systems.

6.11 Upon the termination or expiration of their contract, all Partner, consultants, and temporaries shall return stc assets in their custody, and give their project manager all copies of stc information received or created during the execution of the contract.

6.12 stc data shall not be stored on Partner personal devices and appropriate use of secured filesharing principles, sanctioned by stc authorities should be used during the project or service engagement lifecycle.

6.13 Assets used to process or store stc data and information must be sanitized by the end of the Contract, or by the end of the retention period as stated in the Contract, if defined.

6.14 Partner s should ensure they fully investigate the possibility of using Encryption, Data masking or Data Obfuscation techniques to limit access to stc data by their employees and sub-Partner and avoid localized storage of such information outside of stc approved environments.

7 Cybersecurity Risk management

7.1 Partner is accountable to identify applicable Cyber Risks to Partner 's People, Process and Technologies and is responsible to inform stc Cybersecurity Risk team in a timely manner, along with associated mitigation actions and timelines.

8 Cybersecurity requirements for technology assets

8.1 Partner shall ensure that policies and procedures are in place and followed to prohibit the unauthorized usage of Partners tools, disclosure of knowledge, information, architecture, or configuration relevant to stc 's system.

8.2 Partner shall disable unused services or system features.

8.3 Partner shall ensure that OS is configured in accordance with least privilege to allow only the necessary applications and services to run, and all others are disabled, uninstalled, or otherwise restricted.

8.4 Partner shall ensure that only admin level accounts can reach underlying configurations and are restricted to only those with absolute necessity.

8.5 Partner shall ensure that no admin level accounts are used for day-to-day use.

8.6 Partner shall ensure that all built-in administrator accounts are renamed.

8.7 Partner shall ensure that the built-in Guest account is disabled when not specifically needed.

8.8 Partner shall conduct a configurations' review, secure configuration and hardening and patching before changes or going live.

8.9 Partner shall use only stc authorized software/tools and get approval for any unauthorized binaries from stc Cybersecurity.

9 Cyber security requirements for Identity and Access Management

9.1 Onboarding perquisites

9.1.1 Partner shall provide the complete information required as per Partner profiling template.

9.1.2 Partner shall identify a single point of contact (here after referred to as Partner 's Security Manager) that is suitably qualified and experienced to be responsible in front of **stc** for any security matter.

9.1.3 The Partner 's Security Manager shall be responsible for:

9.1.4 Maintaining regular security reporting to **stc**.

9.1.5 Assuring continuous compliance with **stc** security requirements.

9.1.6 Responsible of any security matter that directly or indirectly impacts **stc** or any of its customers in any way possible.

9.1.7 The Partner shall provide the following information for the security manager and his direct manager:

- Name
- Mobile phone
- Office phone
- Email address

9.1.8 Partner shall ensure that the design of all system components adhere to stc's Cyber Security Architecture Requirements.

9.1.9 Partner 's dispatched team shall sign an NDA with stc to preserve confidentiality of stc information.

9.1.10 Partner shall ensure that policies and procedures are followed to prohibit the unauthorized disclosure of knowledge, information, architecture, or configuration relevant to stc's system.

9.1.11 Partner should confirm that any proposals or contracts signed with stc are in line with the requirements stated in this document.

9.1.12 Partner shall provide a Security baseline (MBSS) for all system components.

9.1.13 Partner shall provide stc with logical and physical infrastructure architecture design in MS Visio.

9.1.14 Partner shall identify any external cybersecurity related compliance requirements as part of any design, development, maintenance, or operation of stc infrastructure.

9.1.15 Partner shall identify, document, resolve, and report any cyber security incident that directly or indirectly impacts stc or any of its customers in any way possible.

9.1.16 The scope of Partner 's incidents that shall be reported to stc covers assets and infrastructures that connect to stc.

9.1.17 Partner shall provide complete information as per stc template for the services/assets that are in-scope of the Partner engagement.

9.2 User Registration and De-registration

9.2.1 Partner Application shall provide Mechanisms and solutions to ensure unique identification of user and information assets should be implemented.

9.2.2 Organizational users (or processes acting on behalf of organizational users). Some common identifiers can be:

- Email address
- Employee code/number

- Name (username, employee name)

9.2.3 stc information assets (devices like workstations, servers, networking, and telco devices) before establishing a connection. Some common identifiers can be:

- Device ID
- MAC address
- TCP/IP address
- Host name

9.2.4 One user should not have more than one application-level accounts

9.2.5 Partner Application should provide user management API to integrate with IDM solution.

9.2.6 Partner Application should expose all user's attributes including last-login-time though API to integrate with IDM solution.

9.2.7 Partner Application should be integrated with other application with secure protocols.

9.2.8 Partner should have the capability to create multiple accounts on his system.

9.3 Authentication, Authorization, and Access

9.3.1 Access to all stc IT systems and applications shall be authenticated.

9.3.2 Systems authenticating user must have the capability to verify identity of the user based on below factors of authentication:

- What the user 'knows' (e.g., a password).
- What the user 'has/possesses' (e.g., an ID badge or a cryptographic key).
- Who the user is (e.g., a fingerprint or other biometric data)?

9.3.3 Partner application shall provide a risk-based decision must be taken to select an appropriate authentication mechanism as well as the choice to use one or more factors of authentication (multi-factor authentication) for an information system.

9.3.4 Partner application shall provide secure protocols must be used for authentication like SAML, WS-Federation, Integrated Windows Authentication – IWA (SPNEGO, Kerberos, and NTLMSSP), LDAPS, IPSec and SSH.

9.3.5 Users and information systems need to re-authenticate in the following situations:

a) when authenticators change
b) when roles change
c) when security categories of information systems change
d) when the execution of privileged functions occurs
e) after a fixed period of time; or periodically

9.3.6 Multi-factor authentication must be used for critical systems, privileged accounts and the systems used to operate and manage these critical systems.

9.3.7 Service accounts for systems and applications must be securely managed with interactive login disabled

9.3.8 Access privileges must be granted based on:

a) Least privilege i.e., a user must not be given any more privilege than necessary to perform a user's job that is defined to a business need.

9.3.9 Secure log-in parameters

a) Suitable authentication techniques should be chosen to substantiate the claimed identity of a user. Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens, or biometric means, should be used.

b) The procedure for logging into a system or application should be designed to minimize the opportunity for unauthorized access. The log-on procedure should disclose the minimum of information about the system or application, to avoid providing an unauthorized user with any unnecessary assistance.

c) Log-on procedures must consider following secure practices:

- Log unsuccessful and successful log-in attempts.
- Must display the timestamp of the previous successful log-on and the details of any unsuccessful log-on attempts on each successful login.
- Must mask the password and not display the entered characters.
- More than 3 unsuccessful login attempts within 5 minutes must result in account locking. These accounts must not be unlocked unless requested by user with justification.
- Must have pre-defined session time-out value or idle-time-out value to systems/application and network devices, respectively.
- Authentication information must not be transmitted in clear text over a network. Suitable cryptographic methods should be used in accordance with CS Cryptographic Standard.
- Concurrent connections must be limited especially in case of business-critical assets.
- Every system, application or a device must show a warning banner mentioning authorized users access and any action (legal or disciplinary) in case of un-authorized access.
- Alert security team of any potential attack or unauthorized activity (like brute force).
- Any detail about the system, application or a device must not be shown until the login is successful and only too users on need-to-know basis.
- Terminate inactive sessions after a defined period of inactivity, especially in high-risk locations such as public or external areas outside the organization's security management or on mobile devices
- Restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

d) Any exception which requires by-pass of secure authentication mechanism (like console connection) must follow a strict approval and authorization by the owner of system, application, or device and also from security team appropriately.

e) Newly instantiated accounts that have been allocated a temporary password must be activated within a five days' interval. Otherwise, the account must be disabled.

9.3.10 Partner shall integrate with stc Identity and Access management solutions whenever applicable.

9.3.11 Partner shall document all accounts (including, but not limited to, generic and/or default) that need to be active for proper operation of the procured product.

9.3.12 Partner 's system shall not allow default passwords, default accounts, anonymous accounts.

9.3.13 Dormant user accounts shall be deleted after a configurable number of days.

9.3.14 Partner 's system shall limit privileges based on users' roles.

9.3.15 Partner shall limit access to database functions to authorized users.

9.3.16 Partner Application should support RADIUS/LDAP/API to integrate with the internal MFA solution for internal users.

9.3.17 Partner Application should support Open-ID Connect/SAML2.0/oAuth2.0 to integrate with SSO solution.

9.3.18 Partner Application should only be accessible through secure protocols such as HTTPS.

9.3.19 Partner Application should show the user last login time while login.

9.3.20 Any device/NE has login page, client, or prompt (CLI) and can be reached through IP network can be integrated with (Network Identity Access Management – NIAM) for Single Sign On.

9.3.21 The other (Network Identity Access Management – NIAM) features like PRA and AM are depending on the device/NE itself if it has a capability for CRUD operations through an API or command line and if they do not have, they need to build it so NIAM can integrate with it.

9.4 **Privileged account management,**

9.4.1 Use of privileged utility programs

a) A list of approved privilege utility programs and scripts should be defined, and only those programs must be executed within **stc** environment and on **stc** systems.

b) Capabilities of the privilege utility programs / scripts should be analyzed and secure ways of using them should be defined through risk assessment.

c) Privilege utility programs must be stored and executed from approved systems only.

d) Access to such programs must be restricted with only few personal having access.

9.4.2 Partner shall limit administrator privilege and root privilege to a limited number of users.

9.5 **Password management.**

9.5.1 Capabilities of a Password management system to be implemented:

a) Force users to change their passwords at the first log-on.

b) Force change of passwords after a defined period

- Corporate accounts – 120 days
- Service accounts – 180 days
- Privilege user accounts – 90 days

c) Allow users to select and change their own passwords.

d) Be able to check the validity of strong and complex password criteria.

e) Automatically prompt for change of password on a periodic basis.

f) Maintain a password history for the user and prevent a password re-use (last 5 passwords).

g) Password history shall be maintained, and the new password must not be identical to previously

used five (5) passwords.

h) The usage of scripting password and hardcoded password must not be used

i) Store and transmit passwords in cryptographically protected form such as hashing functions.

9.5.2 Partner shall provide a configurable account password management system that allows for, but is not limited to, the following (in compliance with stc cybersecurity policy):

a) Minimum Password Length.

b) Password History.

c) Maximum Password Age.

d) Password Complexity

e) Example of password Complexity

f) Account Lockout Duration

g) Account Lockout Threshold

h) Reset Account Lockout counter after specific period

i) Two Factor Authentication

j) Change password at first login attempt must be set to false

k) If No Password Rotation Automation (PRA) is supported. Partner must set password expiry to false

9.5.3 Partner Application password should be encrypted while at rest or in transit.

9.5.4 Partner Application should allow rotating of user's password and should support password rotation though API.

9.5.5 Partner Application should allow discovery of privileged accounts on application and assets through API.

9.5.6 Partner Application should not use hardcoded passwords

9.5.7 Partner should Provide an API for Password Rotation Automation (PRA) Integration.

9.6 **Password Strength and Complexity**

9.6.1 Passwords should be at-least 14 characters long for users that have privileged access (like administrators) and 12 characters long for all other users.

9.6.2 Password should include at-least three combinations of: one upper-case letter, one lower-case letter, one numeral, and one special character.

9.6.3 Few special characters which lead of SQL attacks should not be allowed. For example: ',', ' \', '%' '' and '"" _

9.6.4 To achieve a password of good strength:

- Passwords must not be the known things about user like DOB, DOJ, DOM, birthplace, name of any family member, phone number, etc.
- Password should not simply be a dictionary or a well-known word.
- Avoiding multiple repetition of same character increase the strength of the password.

10 Cyber security Physical access requirements

10.1.1 Partner shall dedicate an access restricted working area for personnel with access to stc network.

10.1.2 Partner is accountable to ensure that its staff and sub-Partner comply to stc Physical Security policies and do not remove or take any stc sensitive information or materials either allocated to them for work purposes or printed on premises.

10.1.3 All stc information is to be retained within stc premises, secured appropriately, and destroyed when no longer required.

11 Cyber security requirements for HR

11.1 **Background Checks**

11.1.1 Partner should ensure that all staff including Outsource employees, Partner, consultants, and sub-Partner working on stc Projects have formal background checks completed including but not limited to:

- Employment History,
- Education Degree,
- Residency
- Regional Law Enforcement Records/history Verification.

11.1.2 Individual screening reports for staff working on stc services should be shared back with stc when requested for formal review and retention.

11.1.3 In case of any conflicts with Data privacy regulations, Partner shall mask PII information and submit the screening reports.

11.2 stc shall ensure that all information assets handed over to the outsourcer during the contract (plus any copies made thereafter, including backups and archives) are duly retrieved or destroyed at the appropriate point on or before termination of the contract.

11.3 Cybersecurity responsibilities and non-disclosure clauses shall be included in Partners personnel contracts and shall be valid during and after the expiry of the employment relation with stc

11.4 In case of policy violations, disciplinary actions, or instances of misconduct by Partner staff or sub-Partner, partner should provide a complete report back to stc authorities forthwith and ensure complete disclosure of any corrective actions taken by the Partner.

11.5 Partner on premise outsourced employees, Partner and consultants shall abide by stc Cybersecurity Policies and Standards.

12 Cyber security Monitoring and Incident response

12.1 Partner should adhere to formal Cybersecurity Incident Response Standards and Policies for stc group and report any potential Cyber Incident to the stc authorities immediately if affecting the stc business.

12.2 Partner shall mandatorily disclose any 'unrelated CS Incidents' within their organizations to stc authorities, in case of a potential reputational impact to stc Business.

12.3 Partner shall provide a list of all log management capabilities that the procured product can generate and the format of those logs. This list shall identify which of those logs are enabled by default.

12.4 Partner shall establish means, procedures and processes that generate logs for enough details to be able to create historical audit for account access activities for a minimum of 1 (one) year.

12.5 Partner root accounts/admin access to logs shall be restricted, and those logs should be encrypted so it cannot be altered including logs backup.

12.6 Partner shall ensure and facilitate the procured systems integration with stc SOC.

12.7 Partner shall ensure that logging facilities and log information are regularly reviewed and protected against tampering and unauthorized access.

12.8 Partner shall ensure that logs are retained and backed up for a minimum duration of 12 month.

12.9 Partner shall provide alternative logging and monitoring solution in case of incompatibility with stc SIEM solutions.

13 Cyber security Remote Access requirements

13.1 Partner shall ensure compliance to all Remote Access Policies, Standards, and Tools within stc, including but not limited to use of Multi-Factor Authentication and other stc mandated controls.

13.2 Partner shall consult Cyber Security Team prior to setting up any remote access connection.

13.3 Partner shall ensure that all unsecure remote access protocols are disabled (Telnet, FTP. etc....)

13.4 Partner shall ensure clear ownership for all remote access accounts.

13.5 Partner should ensure that none of its staff or sub-Partner should be allowed to share remote access credentials and breach of this will be considered a breach of contract by stc.

13.6 Partner should allocate each of partner staff or sub-Partner a registered/stc approved end user device, with the MAC address registered to the single member of the staff for identification and authentication. Failure to do so will result in lack of traceability and the partner organization will be held directly accountable for such breaches.

14 Approved Remote Access Methods

14.1 **Approved methods of remote access in stc are listed in order of preference:**

- Tunneling - a secure communication channel through which information can be transmitted between networks (e.g., Virtual Private Network (VPN)) with no split tunneling.
- Portals - a server that offers access to one or more applications through a single centralized interface that provides authentication (e.g., web-based portal)
- Direct Application Access – accessing an application directly with the application providing its own security (e.g., webmail, https).
- Remote System Control – controlling a system remotely from a location other than **stc**'s internal network

15 Partner Cyber Security Certification: Security Pass Program

15.1 It is the responsibility of the partner to ascertain and meet the requirements of this standard as applicable. Cybersecurity Assessments will be conducted to determine Partner compliance with stc cybersecurity requirements.

15.2 Partners should comply with the applicable cybersecurity requirements set in Appendix E

15.3 Partners that are aiming to conduct business with stc must implement all cybersecurity controls in this standard.

15.4 Partners should refer to the Partner Cybersecurity Control Requirements Guideline to understand the control implementation requirements.

16 Appendix

16.1 Appendix A - Cybersecurity Incident Response Instructions

stc *Incident Reporting Instructions*

1 Notify

1.1 *Initial Notification of Cybersecurity Incident:* The Partner must notify stc cyber security Defense department within one (1) - two (2) hours of discovering any Cybersecurity Incident.

1.2 All notifications must be communicated to cybersecurity defense department via the stc Security email: (DFIR@stc.com.sa)

1.3 *Notify stc of the Cybersecurity Incident*: After the Initial Notification of the Cybersecurity Incident, the Partner must notify stc of all Cybersecurity Incidents stemming from the initial Cybersecurity Incident via the communication method agreed by stc during the initial notification.

2 Review and Identify

2.1 Immediately review all recent changes and modifications to information system users and access privileges for unauthorized modifications.

2.2 Conduct a thorough review of the Partner's information systems for evidence of compromise.

3 Reset Affected Passwords

3.1 Immediately change every password on information systems that are compromised or suspected to be compromised due to the Cybersecurity Incident.

3.2 Document Containment Actions in alignment with Cyber Defense Team.

4 Report (Interim)

Provide stc with reports detailing the Cybersecurity Incident. The Partner must communicate its ongoing efforts to mitigate and resolve the Cybersecurity Incident every twenty-four (24) hours until the time of Cybersecurity Incident resolution.

Please refer to Appendix B.1 for details of the report template.

The Cybersecurity Incident must be classified according to the below classification:

Severity	Description
Low	Cybersecurity Incident that: ▪ Adversely impacts a very small number of systems or individuals ▪ Disrupts a very small number of network devices or segments ▪ Has little or no risk of propagation or causes only minimal

Medium	Cybersecurity Incident that: ▪ Adversely impacts a moderate number of systems and/or people ▪ Adversely impacts a non-critical organization system or service ▪ Adversely impacts a business unit system or service
High	Cybersecurity Incident that: ▪ Threatens to have a significant adverse impact on many systems and/or people ▪ Poses a potential large financial risk or legal liability to the organization ▪ Threatens the confidentiality of data ▪ Adversely impacts an organization system or service critical to the operation of a major portion of stc ▪ Has a high probability of propagating to many systems and causing significant damage or disruption

16.2 Appendix B - Cybersecurity Incident Subsequent Reports and Notifications

B-1 Interim Status Reports

The Partner must provide **stc** cybersecurity defense department with an interim written status report of each Cybersecurity Incident within 24 hours of incident discovery. After the initial report, subsequent Interim Status Reports must be provided to **stc** cybersecurity defense department every 24 hours until the Cybersecurity Incident is resolved. The following report must be used:

Partner Cyber Incident Interim Status Report		**Report No.: #**	
Date:	MM/DD/YYYY	Partner Incident Coordinator Information	
Partner Name:		Name:	
		Email:	
		Phone/Mobile:	
Incident Classification:			
Incident Description:			
Known/Suspected cause:			
Incident Impact:			
Type of information affected:			
Incident Response Activities			
Actions taken:			
Future actions that will be taken:			
Current incident status:			
Expected timeframe for full service restoration:			

B-2 Final Report

1. Business Report

The Partner must provide **stc** cybersecurity defense department with a final written report of any Cybersecurity Incident within three (3) business days of resolution or a determination that the problem cannot be resolved within such time, such report must include:

- The Partner's Name
- The Partner's Incident Coordinator and contact information

- The **stc** Cybersecurity Incident Coordinator
- Date and Time of the Cybersecurity Incident
- Cybersecurity Incident Classification (according to **stc** classification provided in this document)
- Length of Outage and Impact (i.e., Reputational, operational, customer, financial and legal).
- Cybersecurity Incident Executive Overview

2. Technical Report

The Partner must provide **stc** cybersecurity defense department with a final written report of any Cybersecurity Incident within five (5) business days of resolution or a determination that the problem cannot be resolved within such period, such report must include:

- The Partner's Name
- The Partner's Incident Coordinator and contact information
- The **stc** Cybersecurity Incident Coordinator
- Date and Time of the Cybersecurity Incident
- Cybersecurity Incident Classification (according to **stc** classification provided in this document)
- Impact and Length of Outage
- Cybersecurity Incident Executive Overview including the Cybersecurity Incident impact (i.e., Reputational, operational, customer, financial and legal).
- Cybersecurity Incident Details:
  - List of individuals and other Partners that were involved with any aspect of the Cybersecurity Incident handling
  - How/when the Cybersecurity Incident was initially detected
  - How/when the Cybersecurity Incident was initially reported to **stc**
  - Description of what resources/services were impacted
  - Description of Cybersecurity Incident's impact to **stc** (volume and type where applicable)
  - Containment - How was the Cybersecurity Incident contained
  - Root Cause - What was the cause for disruption
  - Corrective action during the Cybersecurity Incident – What steps were taken to reduce exposure during the Cybersecurity Incident (in most cases, there are interim steps taken to reduce exposure, e.g., Filtering, rerouting services, etc.)
  - Permanent corrective actions/preventative measures – What permanent corrective actions have been put in place because of this Cybersecurity Incident
  - Conclusion

16.3 Appendix C - Auditing Events

Information Systems must be capable of auditing the events listed below.

NO	Event Type
1	System starts
2	System shutdown
3	System restart
4	Successful login attempts (Logon Types must be included)
5	Failed login attempts
6	Service creation
7	Addition of user account
8	Deletion of user account
9	Escalation/modification of account privileges
10	Modification of security configuration/policies
11	Deletion of user accounts
12	Activities of privileged accounts
13	Logs cleared
14	Attempt/Failure to access removable storage
15	Session connected, reconnected, and disconnected
16	Plug and Play driver install attempted (System Log)

NO	Event Attributes
1	Timestamp
2	User ID
3	Event name
4	Event category
5	Event severity
6	Host name
7	Source IP address
8	Destination IP address
9	Source Port
10	Destination Port

NO	Event Type	Event Attributes
1	**web access logs / error logs for webservers.** These events include changes to systems or applications, changes to data (creation and destruction) and application installation and changes.	▪ Admin Activity audit logs (Application) ▪ Data Access audit logs ▪ Application Event audit logs
2	**Authentication, Authorization, and Access**	successful and failed authentication and authorizations, system access, data access and application access.

16.4 Appendix D - Securing Confidential Documents Instructions

Documents containing confidential information must be password-protected at all times. The following instructions must be followed to ensure the security of these documents:

- These documents must only be shared with limited individuals who are part of the work specified in the Contract.
- Passwords to unlock these documents:
  - Must never be stored.
  - Must never be shared in the same communication method (e.g., email) as the documents.
  - Must be communicated to the recipient(s) over the phone, in person or via SMS text message.
  - Must be in line with the password protection measures stated in Control Number "AC-2" in this Standard in agreement with a **stc** eligible recipient of the document.

16.5 Appendix E – Security Pass Cybersecurity Controls

This section identifies the required cybersecurity controls that are among the best practices in Cybersecurity such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) in which this Standard is aligned to.

CNTL #	Control Name	NIST CSF Ref.
IDENTIFY		
Asset Management (AM)		
SP-1	The Partner must have policies and processes to classify information in terms of its value, criticality, confidentiality, and sensitivity.	ID.AM-5
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.	ID.AM-6
Governance (GV)		
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.	ID.GV-1 ID.GV-2
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.	ID.GV-1 ID.GV-2
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.	ID.GV-1 ID.GV-2
Risk Assessment (RA)		
SP-6	The Partner must conduct annual Penetration Testing on their IT infrastructure.	ID.RA-1, ID.RA-2 ID.RA-5
Risk Management Strategy (RM)		
SP-7	The Partner must have a Risk Management process in place to identify, assess and remediate Risks to information systems.	ID.RM-1
PROTECT		
Access Control (AC)		
SP-8	Users accessing information systems must be issued unique user logins and passwords. Generic accounts must not be allowed.	PR.AC-1 PR.AC-4

CNTL #	Control Name	NIST CSF Ref.
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 5 minutes of inactivity.	PR.AC-1
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.	PR.AC-1
SP-11	Permanent security badges must be issued to Partner employees. Personnel must wear picture identification badges always.	PR.AC-2 DE.CM-2
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	PR.AC-2 PR.DS-1
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.	PR.AC-4
SP-14	The Partner must dedicate an access restricted working area for personnel with access to stc network.	PR.AC-5
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.	PR.AC-5
SP-16	The server and workstation subnets must be segmented and access between them is restricted and monitored on a regular basis.	PR.AC-5
SP-17	Servers accessible from the Internet must be placed in a DMZ (i.e., perimeter network) with restricted access to internal subnets.	PR.AC-5
SP-18	Remote connections to information systems at the Third Parties location must be authorized, monitored, and have two-factor authentication.	PR.AC-3
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.	PR.AC-3 PR.DS-2
SP-20	Partner must not use traffic anonymizers, proxies or sites redirectors when accessing stc services.	PR.AC-3 PR.AC-5

CNTL #	Control Name	NIST CSF Ref.
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.	PR.AC-1
Awareness and Training (AT)		
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	PR.AT-1 PR.AT-2 PR.AT-3
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.	PR.AT-1 PR.AT-2 PR.AT-3
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.	PR.AT-1 PR.AT-2 PR.AT-3
Data Security (DS)		
SP-25	All Partner devices such as systems, workstations and laptops must be password protected.	PR.DS-1
SP-26	The "Remember Passwords" feature must be disabled in web browsers.	PR.DS-2
SP-27	Backup media must be secured to block/inhibit unauthorized physical access.	PR.DS-1, PR.DS-5
SP-28	Partner workstations, laptops and servers must be regularly updated with operating system (OS), software and applets patches (i.e., Adobe, Java etc.)	PR.DS-1, PR.DS-5
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.	PR.DS-1, PR.DS-5
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).	PR.DS-2
SP-31	The Partner must employ encryption mechanisms, using at least AES encryption algorithm, and 256 bits key, on all devices or storage media hosting sensitive data per the Partner's assets tiering policy.	PR.DS-1
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.	PR.DS-5

CNTL #	Control Name	NIST CSF Ref.
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.	PR.DS-5
SP-34	Partner must implement Sender Policy Framework (SPF) technology on the mail server.	PR.DS-5
SP-35	Documents containing stc Confidential Information, or higher classification, must be encrypted and password- protected at all times.	PR.DS-1 PR.DS-2
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.	PR.DS-5
Information Protection Processes and Procedures (IP)		
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.	PR.IP-1
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.	PR.IP-4 PR.DS-1
SP-39	The Partner must employ a sanitization process before any Assets are loaned, donated, destroyed, transferred, or surpluses. The process must be aligned to industry best practices such as NIST 800-88.	PR.IP-6
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.	PR.IP-9
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: 1 Equipment failure. 2 Disruption of power supply or communication. 3 Application failure or corruption of database. 4 Human error, sabotage, or strike. 5 Malicious Software attack. 6 Hacking or other Internet attacks. 7 Social unrest or terrorist attacks. 8 Environmental disasters. 9 Emergency contact information for personnel.	PR.IP-9
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.	PR.IP-9

CNTL #	Control Name	NIST CSF Ref.
SP-43	Partner must conduct Business Continuity drills at least annually.	PR.IP-9
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.	PR.IP-11
Protective Technology (PT)		
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.	PR.PT-1
SP-46	The Partner must retain all audit logs from information systems storing, processing, or transmitting stc data for one (1) year.	PR.PT-1
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.	PR.PT-3 PR.DS-1
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.	PR.PT-3
SP-49	Firewalls must be configured and enabled on endpoint devices.	PR.PT-4
Protective Technology (PT)		
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.	PR.PT-4
SP-51	Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) must be implemented at the network perimeter.	PR.PT-4
SP-52	Signatures of firewalls and IDS and IPS must be up to date.	PR.PT-4
DETECT		
Anomalies and Events (AE)		
SP-53	Partner must have an incident response procedure	DE.AE-1 DE.AE-2
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	DE.AE-3
Continuous Monitoring (CM)		

CNTL #	Control Name	NIST CSF Ref.
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.	DE.CM-2
SP-56	Non-authorized devices (such as personal devices and mobile phones) must not be used to store, process or access Assets.	DE.CM-7 PR.DS-5
SP-57	Monthly Vulnerability scans must be conducted to evaluate configuration, Patches, and services for known Vulnerabilities.	DE.CM-8
SP-58	Physical access to the facility where information systems reside must be restricted and monitored.	DE.CM-3
SP-59	Information systems must log auditable events as stated in Appendix C.	DE.CM-1
RESPOND		
Communications (CO)		
SP-60	Incident management policy and procedures must be documented, maintained, and communicated to management and appropriate team members.	RS.CO-1 RS.CO-4 RS.AN-1 RS.AN-2 RS.AN-3 RS.AN-4 RS.MI-1 RS.MI-2 RS.IM-1, RS.IM-2
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.	RS.CO-2
Analysis (AN)		
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.	RS.AN-2 RS.AN-3 RS.AN-4
SP-63	The Partner must track, classify, and document all Cybersecurity Incidents.	RS.AN-1
Mitigation (MI)		

CNTL #	Control Name	NIST CSF Ref.
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.	RS.MI-3

17 Attachments

DATA%20PROTECTION%20AGREEMENT%

Data%20Processing%20Agreement-(Eng-