SABIC CyberTrust Standard

Version 1.0

Disclaimer
This is a controlled document for business use by SABIC and its' business partners only. This document cannot be changed or distributed with any modification unless SABIC approves a new version.

Contents

1. DEFINITIONS

The following terms and abbreviations have been defined for use within this document:

Term	Definition
Access Management Policy	A policy that defines the required access control measures to all the information systems and applications to protect the privacy, security, and confidentiality of information technology resources.
Advanced Persistent Threat	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives. The advanced persistent threat pursues its objectives repeatedly over an extended period.
Anti-Malware	Software that is designed to detect, and remove, block, or contain various forms of malicious software.
Asset	Anything that has value to an organization, including but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software, virtual computing platform, and related hardware.
Audit Log	Chronological record of information system activities providing an independently verifiable trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.
Backup	A backup, or data backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.
Cloud computing	It is a model that enables convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud models are composed of five Essential Characteristics: On-demand self-service, broad network access, Resource pooling, rapid elasticity, and measured service. There are three types of cloud computing services delivery models: • Cloud Software as a Service (SaaS). • Cloud Platform as a Service (PaaS). • Cloud Infrastructure as a Service (IaaS).
Consulting Services	Services provided by a professional advisory team where consultants review and analyze client business data and documents, which may contain sensitive and confidential data, and offer advice, benchmarks, and use their expertise to recommend best practice or help businesses based on their individual requirements.
Contract	An agreement between parties creating mutual obligations enforceable by law.
Cybersecurity	The information security requirements needed to support the protection of confidentiality, integrity, and availability of Assets.
Cybersecurity Acceptable Use	It is a policy stipulating constraints and practices that a System User must agree to for access to a corporate network, the internet or other resources. It states what a System User can and cannot do when using computers and computing resources.
Cybersecurity Assessment	Assessment conducted by SABIC to ensure that the Supplier is in full compliance with the Supplier Minimum Cybersecurity Requirements included in this document and any Contract.

Term	Definition
Firewall	Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
Industrial Control System (ICS)	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.
Logical access	Providing an authorized System User the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A Logical access control system requires validation of an individual's identity through some mechanism such as a personal identification number, smartcard, username and password, biometric, or other token.
Outsourcing	Business practice in which certain functions required by the business are performed by outside parties on a contract basis rather than the business's employees
Managed Services	Professional services that are provided on subscription basis to offload some professional IT and cybersecurity operations. This includes products, solutions, software, and hardware
Multi-Factor Authentication	Method of authenticating a system user whereby at least two factors are verified. These factors include something the System User has (such as a smart card or dongle), something the System User knows (such as a password, passphrase, or PIN), or something the System User has or does (such as fingerprints and other biometric elements).
Operational Technology (OT)	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.
Patch	A piece of software designed to fix operating system or software programming errors and Vulnerabilities
Phishing	Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
Purchase Order	The document, including any attachments thereto, issued by Purchaser to order goods and/or services from Supplier.
Sanitize	The action of permanently removing all data and/or licensed software, through overwriting or degaussing methods, from an Asset before that Asset is disposed, loaned, destroyed, donated, transferred, or surpluses.
Saudi Aramco	Saudi Arabian Oil Company, a joint stock company incorporated under the laws of the Kingdom of Saudi Arabia, having its head office located at P.O. Box 5000, Dhahran, 31311, Kingdom of Saudi Arabia, registered with the Commercial Register under number 2052101150, and having a share capital of 60,000,000,000 Saudi Riyals fully paid.
SAUDI BASIC INDUSTRIES CORPORATION (SABIC)	SAUDI BASIC INDUSTRIES CORPORATION, a joint stock company incorporated under the laws of the Kingdom of Saudi Arabia, having its head office located at P.O. Box 5101, Riyadh, 11422, Kingdom of Saudi Arabia, registered with the Commercial Register of Riyadh on 14 Muharram 1397H corresponding to 4 January 1977 under number 1010010813, and having a share capital of 30,000,000,000 Saudi Riyals fully paid.

Term	Definition
Sender Policy Framework	Email-validation system that allows domain owners to publish a list of authorized IP addresses or subnets to detect and block email spoofing, and reduce the amount of spam, fraud and Phishing.
Social Engineering	A manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these "human hacking" scams tend to lure unsuspecting System Users into exposing data, spreading malware infections, or giving access to restricted systems.
Staff Augmentation	The service provides people to augment the company staff with skill needed. The organization's augmented staff will be managed directly by the company, as if they are employees
Supplier	The legal entity specified in the relevant Purchase Contract as the supplying Party.
Supplier Environment	Supplier collection of computers, data storage devices, workstations, software applications, and networks that support the processing and exchange of electronic information.
System Integration	The service to support the creation a complex information system that may include designing or building a customized architecture or application, integrating it with new or existing hardware, packaged and custom software, and communications.
System Users	Supplier employees, contractors and others who have access to the Supplier information systems.
Telework System	Any technical system means or tools and its related components that are used by the organization to enable employees to perform their job duties in a place other than the official workplace. Examples include virtual meeting systems, collaboration systems, file sharing, virtual private network (VPN), remote access systems, and other systems used in the work environment.
Data Loss Prevention (DLP)	Set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. DLP software classifies and monitors data to protect it both in transit and at rest, and can enforce data security policies to prevent unauthorized data transfers.

2. PURPOSE

SABIC CyberTrust Standard defines the cybersecurity requirements for SABIC suppliers falling under the classifications described in *Section "3. Scope"* of this standard, or volunteered suppliers that do not fall under the classifications, to protect SABIC from associated cybersecurity threats, and to strengthen suppliers' cybersecurity posture.

3. SCOPE

This document applies to new or existing Suppliers falling under the classifications in the table below and to Suppliers that have access to SABIC data. Other Suppliers can volunteer to comply with this Standard.

Additional to the general requirements, specific cybersecurity requirements are defined for suppliers classified under the below classifications:

Type of Service	Code	Description
Network Connectivity	**NC**	Suppliers who require network connectivity to SABIC to provide its services including telecom-based services.
Cloud Computing Services (IaaS, PaaS, SaaS & Faas)	**CCS**	The Supplier provides cloud computing services: • Cloud Infrastructure as a Service (IaaS). • Cloud Platform as a Service (PaaS). • Cloud Software as a Service (SaaS). • Function as a service (Faas).
Outsourcing and Managed Services	**OMS**	Suppliers providing outsourcing and/or managed services including services and infrastructure such as data centers, co-location centers, and offline backup centers.
Consultancy Services	**CS**	Suppliers providing consultancy services with access to SABIC's classified data (i.e., financial data, strategic projects, confidential and strictly confidential data).
Software Management	**SM**	Suppliers providing custom software development and/or maintenance or packaged solutions.
OT/ICS products and services	**OT**	Suppliers providing OT product and/or services.

4. CONFLICTS AND DEVIATIONS

In the event compliance with an applicable cybersecurity requirement included in this document is not technically possible, a waiver must be requested explaining the compensating control(s) applied. The waiver request will be analyzed by the auditor and raised to SABIC for approval.

5. REVISION

This Standard will be reviewed, and updated annually or as required, by SABIC Cybersecurity department, to ensure that it continues to meet the business requirements. Updates to the cybersecurity requirements will be communicated to the Suppliers where a significant change is made.

Before obtaining a new certification or renewing an existing one, it is advisable to download the required documents from SABIC's website.

6. CYBERSECURITY REQUIREMENTS INSTRUCTIONS

Suppliers falling under the classifications described in *Section "3. Scope"* of this standard and Suppliers that have access to SABIC data must fully comply with the cybersecurity requirements specified in Section "General Cybersecurity Requirements" of this document. Additionally, based on the type of service specified in their contracts, must also ensure adherence with the applicable cybersecurity requirements specified in *Section "7.2 Specific Cybersecurity Requirements"* of this Standard.

Suppliers not falling under the classifications and don't have access to SABIC data can voluntary comply with the "General Cybersecurity Requirements" in order to obtain the SABIC CyberTrust certification.

7. SUPPLIER CYBERSECURITY REQUIREMENTS

7.1 GENERAL CYBERSECURITY REQUIREMENTS

Classified and volunteered suppliers must fully comply with all Cybersecurity requirements set forth in the table below.

Control ID	Requirement
GOVERN	
Policies, Processes, and Procedures (GV.PO)	
CT-01	**Information security management** Suppliers must have defined policies for information security, approved by their management, and communicated to the people with access to their information systems.
IDENTIFY	
Improvement (ID.IM)	
CT-02	**Self-assessments** Suppliers will perform, at minimum, a self-assessment of their operational resilience and Cybersecurity practices in order to identify and appropriately manage potential risks. The self-assessment must include, at minimum, all the requirements included in this document. The self-assessment must be repeated at yearly intervals (or when requested by SABIC).
Asset Management (ID.AM)	
CT-03	**Asset Management** SABIC Assets associated with information processing facilities managed by the Supplier must be identified and an inventory of these Assets must be drawn up and maintained by the Supplier.
PROTECT	
Identity Management, Authentication, and Access Control (PR. AA)	
CT-04	**Access control management** Supplier must have a defined, documented and enforced Access Management Policy for physical and Logical access to networks, systems, and applications in Supplier Environment that processes, accesses, or stores SABIC 's data. At least the Access control management must include: • The access rights granting, changing, and disabling based on documented and authorized approvals. • A process implemented to ensure the disabling of account of personnel no longer on employment or contracted. • The periodical review of access rights to ensure that access is fit for purpose. In addition, it is recommended to implement the following password security requirements. • Password minimum length of 8 characters and complexity rules. • Password expiry set not less than 90 days. • Account lockout threshold set to 10 attempts (or less). • No password sharing allowed.

Control ID	Requirement
	Platform Security (PR.PS)
CT-05	**Physical security perimeter** Supplier must define and implement the security perimeters of their Environment to protect key systems/services and physical assets.
CT-06	**Media protection** Supplier must protect both paper and electronic information or any other media storing SABIC's data, by limiting access to information on those media to the authorized System Users and Sanitize or destroy information system media before disposal or release for reuse.
CT-07	**Personnel security** Suppliers must apply preventive measures confirming the adequacy and integrity of their System Users involved in the provision of services to SABIC. These measures must, at minimum, include the verification of their references and identity and the employee's agreement for proper use of information systems. The Supplier must report all changes related to System Users with access to SABIC's information systems so that their access authorization can be updated by SABIC accordingly. The Supplier must have formal procedures for off-boarding employees and contractors. Off-boarding procedures must include the return of Assets, and removal of all associated access rights.
	Awareness and Training (PR.AT)
CT-08	**System Users training** Supplier must provide and require all System Users to take a yearly mandatory Cybersecurity awareness training that addresses acceptable use and good computing practices. Training must address at least the following topics: • Cybersecurity Acceptable Use. • Internet and social media security. • Social Engineering and Phishing emails. • Confidentiality and not sharing credentials (e.g., user/password). • Information security policies.
	Technology Infrastructure Resilience (PR.IR)
CT-09	**Email service protection** The Supplier must protect its email service with at least the following: • Analyzing and filtering email messages (specifically regarding Phishing and spam) using up-to-date email protection techniques • Multi-Factor Authentication for remote and webmail access to email service. • Email archiving and Backup. • Secure management and protection against Advanced Persistent Threats. • Validation of the Supplier email service domains (e.g., using Sender Policy Framework).
CT-10	**Patching** Supplier technology Assets and systems must be regularly updated with the operating system (OS), software and applications Patches provided by their manufacturer according with industry best practices.
CT-11	**Anti-Malware** Supplier technology Assets must be protected with Anti-Malware software. Updates must be applied daily, and full system scans must be performed at least every two weeks. In case of virus/malware detection, the virus/malware must be eradicated promptly, and the affected systems restored to a clean status.

Control ID	Requirement
CT-12	**Network controls** Networks in the Supplier Environment shall be managed and controlled to protect information in systems and applications. Network controls shall be deployed by means of Firewalls and other network security technologies that includes Intrusion Detection Systems (IPS) or Intrusion Detection Systems (IDS) and acting as network policy enforcement points.
DETECT	
Continuous Monitoring (DE.CM)	
CT-13	**Audit and accountability** Supplier must create and maintain information system Audit Logs needed to allow the analysis, investigation, and reporting of unauthorized, or inappropriate information system activity in the Supplier Environment and ensure that the actions of individual information System Users can be attributed to those System Users.
RESPOND	
Incident Management (RS.MA)	
CT-14	**Incident response** Supplier must have an incident handling process for information systems in the Supplier Environment, which includes the preparation to detect, analyze, contain, recover and response to incidents.
Incident Analysis (RS.AN)	
CT-15	**Incident categorization** The supplier must define a clear process of how incidents are categorized based on the impact it could leave.
RECOVER	
Incident Recovery Communication (RC.CO)	
CT-16	**Supplier incident reporting** The Supplier must notify and report to SABIC any adverse situation or Cybersecurity incident that occurs in the Supplier Environment, affecting any networks, systems or applications that process, access, or store SABIC's data. The notification must be made as soon as practicable, but **no later than twenty-four (24) hours** after the Supplier becomes aware of it or should have become aware of it. The Supplier must make the notification to SABIC using the following channel: Email: CyberSecurityCenter@SABIC.COM

7.2 SPECIFIC CYBERSECURITY REQUIREMENTS

Suppliers falling under one or more of the classifications described in *Section "Scope"* of this standard, based on the type of service specified in their contracts, must also ensure adherence with the specific cybersecurity requirements along with the general cybersecurity requirements described herein based on their classification(s). The code used to identify the classifications are as below:

Type of Service or Good	Code
Network Connectivity	NC
Cloud Computing Services (IaaS, PaaS, SaaS & Faas)	CCS
Outsourcing and Managed Services	OMS
Consultancy Services	CS
Software management	SM
OT/ICS products and services	OT

Control ID	Requirement	NC	CCS	OMS	CS	SM	OT
GOVERN							
Risk Management Strategy (GV.RM)							
CT-17	The Supplier must maintain a Cybersecurity risk management and mitigation program, with clear roles & responsibilities, processes, risk appetite and tolerance, risk strategy, and Third Party Risk Management.	✓	✓	✓		✓	✓
Policies, Processes, and Procedures (GV.PO)							
CT-18	The Supplier must have policies and processes to classify information in terms of its value, sensitivity, criticality, confidentiality and regulatory requirements.	✓	✓	✓	✓	✓	✓
Roles, Responsibilities, and Authorities (GV. RR)							
CT-19	The Supplier must have employee(s) whose primary responsibility is Cybersecurity. Responsibilities of those personnel must include maintaining the security of information systems and ensuring compliance with existing policies.	✓	✓	✓		✓	✓
CT-20	The Supplier must conduct background check (screening/vetting) on Employees viewing or/and processing SABIC's confidential and strictly confidential	✓	✓	✓	✓	✓	✓
IDENTIFY							
Asset Management (ID.AM)							
CT-21	The Supplier must follow an established Secure development Life Cycle (SDLC) for the Software and product development. The SDLC should comply with applicable best practice guidelines. SDLC should incorporate vendor-specific development best practices to ensure applications are built with the recommended security guidance from the vendor.	☒	✓			✓	✓

Control ID	Requirement	NC	CCS	OMS	CS	SM	OT
CT-22	Supplier must use Secure-by-design principles as part of security architectural designs for OT/ICS products. Secure-by-design principles include establish secure defaults, minimize attack surface area, fail securely, defense in depth, least privilege, separation of duties, keeping security simple and avoid security by obscurity.						✓
CT-23	The Supplier must inventory all third-party software components (whether commercial, free, or open-source software) used in the Software development and provide such inventory to SABIC upon request. Supplier must assess whether any such components have any security defects or vulnerabilities that could lead to a Security Incident.					✓	
Risk Assessment (ID.RA)							
CT- 24	The supplier must conduct risk assessment to identify potential threats and mitigation plans of the identified risks should be well documented.	✓	✓	✓	✓	✓	✓
CT-25	The Supplier must perform a regular vulnerability scanning using trusted vulnerability management technologies.	✓	✓	✓	✓	✓	✓
CT-26	The Supplier must conduct at least annual Penetration Testing on its IT infrastructure systems and internet facing applications by reputed external party.	✓	✓	✓	✓	✓	✓
Improvement (ID.IM)							
CT-27	The personnel with access to OT/ICS assets, besides the general cybersecurity training and awareness, must go through an OT/ICS cybersecurity awareness and training program. The program must include, at a minimum, the following: customized training, qualifications, knowledge, and professional skillsets related to the OT/ICS assets cybersecurity.						✓
CT-28	The Supplier must have a process in place to guarantee that a non-disclosure agreement between contracted employees of the Supplier and the Supplier is signed before access to SABIC systems and/or premises is granted.	✓	✓	✓	✓	✓	✓
PROTECT							
Identity Management, Authentication, and Access Control (PR. AA)							
CT-29	System Users must have unique user logins and passwords for applications and systems. Generic accounts must not be allowed, unless explicitly approved, restricted, and controlled.	✓	✓	✓	✓	✓	✓
CT-30	All privileged accounts must be limited, justified, and reviewed on regular basis.	✓	✓	✓		✓	✓
CT-31	Multi-factor authentication must be enforced on all privileged accounts access including remote access to information systems and applications.	✓	✓	✓		✓	✓
CT-32	The Supplier must support identity federation services.		✓			✓	
Platform Security (PR.PS)							
CT-33	The Software must have the capability to segregate different data typology processed.					✓	
CT-34	The Software must have the capability to provide authorization based on roles.					✓	
CT-35	The Software must support multi-factor authentication for users.					✓	
CT-36	The Software must have the capability to segregate users' accessible data.					✓	

Control ID	Requirement	NC	CCS	OMS	CS	SM	OT
CT-37	Network connections to information systems and applications at the Supplier location must be authorized and monitored.	✓	✓	✓	✓	✓	
CT-38	The cryptographic technologies used by the product must be aligned with the applicable national regulations.	✓	✓	✓		✓	✓
CT-39	The Supplier must implement sufficient mechanisms to protect data-in-transit. Data-in-transit should be encrypted with strong, approved algorithms. End-to-end encryption should be enforced where applicable using VPN and/or TLS capable connectivity solutions with secure key exchange and forward-secrecy capability.	✓	✓	✓		✓	✓
CT-40	Encryption keys and certificates must be managed in a secure manner.	✓	✓			✓	✓
CT-41	The Supplier must implement data-at-rest encryption mechanisms, using at least AES-128 encryption algorithm, on all devices or storage media hosting sensitive data.	✓	✓	✓		✓	✓
CT-42	Wireless networks accessing information systems must use strong encryption for authentication and transmission, such as WPA2 or WPA2 Enterprise.	✓		✓			
CT-43	Creation of tunnels must be based on certificates with automation of tunnel creation and key rotation for each tunnel.	✓	✓	✓		✓	
CT-44	The Supplier must provide secure session management including session authenticity, lockout, and timeout termination.		✓				
CT-45	The Supplier must have network controls deployed such as firewalls, network segmentation, network access control, Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) and DoS filtering.	✓	✓	✓		✓	
CT-46	The Supplier must implement a device control mechanism (Endpoint Security) on Assets that are used to receive, store, process or transmit SABIC data.	✓	✓	✓	✓	✓	
CT-47	The Supplier must have and apply a secure baseline configuration which should be established following applicable best practice guidelines (e.g., CIS) for all underlying assets used to provide the agreed service.	✓	✓				
CT-48	The Supplier must conduct periodic vulnerability scans to evaluate configuration, Patches, and services for known Vulnerabilities.	✓	✓	✓		✓	✓
CT-49	The Supplier must implement 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.	✓	✓	✓		✓	✓
CT-50	The Supplier must retain all audit logs from information systems and applications storing, processing, or transmitting SABIC data for one (1) year, as per local and international laws and regulations (whichever is greater) depending upon the type of data being collected.	✓	✓	✓		✓	✓
CT-51	The Supplier must ensure the isolation of tenants. The SABIC's environments/data (specifically virtual server if applicable) must be separated from other customer environments/data hosted at the cloud services provider.		✓				
CT-52	The Supplier must have the capability to restrict the storage of the customer data to specific countries or geographical locations in compliance with applicable laws and regulations.		✓				
CT-53	The supplier must ensure the implementation of a data loss prevention (DLP) technology.	✓	✓	✓	✓	✓	✓

Control ID	Requirement	NC	CCS	OMS	CS	SM	OT
Technology Infrastructure Resilience (PR.IR)							
CT-54	The Supplier must ensure that physical assets are adequately secured and that access to the physical assets as well as SABIC's data is restricted to authorized personnel only. Access in such cases must be documented, and compliant with any applicable legal requirements.	✓	✓	✓			
CT-55	The Supplier must implement data validation on all input fields for applications or Cloud Services used by SABIC to only accept input with valid data type, syntax, length range, sanitized, accurate, well-formed, and adheres to defined constraints		✓			✓	
CT-56	Access to the Internet must be restricted by Content-filtering technologies to block: • Malicious and suspicious websites. • Personal and non-company email services. • Personal and non-company approved public cloud services.	✓	✓	✓	✓	✓	
CT-57	Physical security procedures defined and followed that address the control of physical access, environmental protection, equipment maintenance, equipment siting, visitor management etc.	✓	✓	✓		✓	
CT-58	Access to sensitive areas (server location, tape library, computer room, etc.) must be physically restricted to authorized personnel only; wherever applicable physical access control must be implemented.	✓	✓	✓		✓	
CT-59	The facilities must be protected against fire, water damage, vandalism, and other threats known or likely to occur at their geographical locations.	✓	✓	✓		✓	
CT-60	Facilities and server rooms must be monitored via a Closed-Circuit Television (CCTV) system on a 24/7 basis. All video surveillance data must be protected from unauthorized disclosure and modification and maintained for at least ninety (90) days or otherwise in accordance with the local/regional regulations.	✓	✓	✓		✓	
CT-61	Uninterruptible Power Supplies (UPS) and surge protector must be used to provide short-term and long-term power when the power fails and to protect information systems from voltage spikes and reductions.	✓	✓	✓		✓	
CT-62	The Cloud service provider must establish mechanisms to automatically identify equipment using connection authentication (cryptographic based mechanisms that get verified after establishing a connection between the communicating services).		✓				
CT-63	The Supplier must return the SABIC data in a usable format upon service completion		✓			✓	✓
CT-64	The Supplier must provide security documentation for any equipment or services under request by SABIC.		✓				
CT-65	The Supplier must use a source code control system that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files					✓	
CT-66	Supplier system development environments, including testing environment and integration platforms, must be protected.		✓			✓	✓

Control ID	Requirement	NC	CCS	OMS	CS	SM	OT
CT-67	The Supplier must use a build process that reliably builds a complete distribution from source. This process must include a method for verifying the integrity of the software delivered to Client, such as signing with a certificate from an industry recognized Certificate Authority.					✓	
CT-68	The Supplier must apply, test, and validate the appropriate patches and updates and/or workarounds on a test version of the application before distribution.					✓	
CT-69	The Supplier must provide periodic security patches certified by it and upgrades and implementation guidance or recommendations with respect to cybersecurity.					✓	✓
CT-70	All media must be inventoried and labelled as per the classification level. Inventory audit should be used to avoid unknown or unresolved discrepancies in tape inventories in order to find the information needed to get up and running in the event of a disaster.	✓	✓	✓			
CT-71	Backup media must be secured to block/inhibit unauthorized physical access.	✓	✓	✓		✓	
CT-72	Supplier must establish and follow regular procedures for backup of critical systems and SABIC's data, software, and websites.	✓	✓	✓			
CT-73	Backup stored at an off-site location must be encrypted using at least AES encryption algorithm, and 128 bits key.	✓	✓	✓		✓	
CT-74	Clear desk and clear screen policy must be enforced in the organization.	✓		✓	✓	✓	
CT-75	The Supplier must monitor Technology Assets, Systems, and applications to identify unauthorized access, or unauthorized activity.	✓	✓	✓			
CT-76	The Supplier must conduct an analysis of software errors, most common programming errors, vulnerabilities, risks a threat as early as possible during the software lifecycle. The Supplier must share with SABIC all security-relevant information regarding the vulnerabilities, risks, threats, and mitigated steps taken.					✓	
CT-77	The Supplier must ensure that errors and events within the application that may be the result of failures, crashes, unauthorized access attempts or other indicators of potential compromise, are appropriately recorded in a log file conforming to industry standards.					✓	
CT-78	The Supplier must perform security scans (with the most current signature files) to verify that the system has not been compromised during the testing phase or it has open vulnerabilities. The Supplier must provide to SABIC written documentation of the results of the scans and tests it has performed along with a mitigation plan. These vulnerabilities must be mitigated within a pre-negotiated period.					✓	
CT-79	All physical access control logs periodically reviewed and retained as per retention requirements.	✓	✓	✓		✓	✓
CT-80	Systems' logs and critical files must be protected from unauthorized access, tampering, illegitimate modification and/or deletion.	✓	✓	✓		✓	✓
CT-81	Records kept of all suspected or actual faults and all maintenance activities performed on equipment's Is the maintenance must be carried out by authorized personnel only.	✓	✓	✓			
DETECT							

Control ID	Requirement	NC	CCS	OMS	CS	SM	OT
Continuous Monitoring (DE.CM)							
CT-82	The remediation of newly discovered critical vulnerabilities presenting significant risks must be performed in a timely manner: • Critical Risk: immediate correction up to fourteen (14) calendar days of critical vendor patch release, notification from SABIC, or discovered security breach whichever is earlier. • High Risk: within one (1) month of vendor patch release or discovered security breach whichever is earlier. • Medium and Low Risk: within three (3) months of discovery.	✓	✓	✓		✓	✓
CT-83	The supplier must be continuously monitoring cybersecurity events through a security incident and event management process.	✓	✓	✓	✓	✓	✓
Adverse Event Analysis (DE.AE)							
CT-84	Suppliers must periodically aggregate and correlate data from multiple systems and critical applications such as Firewalls, IDS/IPS, and anti-virus in a central repository for event monitoring and analysis purposes.	✓	✓	✓			
CT-85	The Supplier must have a Disaster Recovery Plan (DR Plan) which is documented, maintained, tested, and communicated to appropriate parties. The DR Plan should address the recovery of Assets and communications following a major disruption to business operations.	✓	✓	✓			
RESPOND							
Incident Management (RS.MA)							
CT-86	The Supplier must have security mechanisms in place to achieve resilience requirements in normal and adverse situations and ensure high availability of its services. This includes having sufficient capacity available.		✓	✓			
CT-87	Procedures for the backups of the provisioned solution and SABIC's data must be established, conducted, maintained, and tested on a regular basis. SABIC can define more specific requirements for backup in the Scope of Work.	✓	✓	✓	✓		
Incident Response Reporting and Communication (RS.CO)							
CT-88	Supplier must have an Incident Response capability that includes preparation, detection and analysis, containment, eradication, recovery, documentation and preservation of evidence, communication protocols and lessons learned.	✓	✓	✓			
CT-89	Documented Security Incident Response process covering physical security incidents.	✓	✓			✓	✓

To be certified to provide cloud services or outsourcing and manage services to SABIC Saudi-Based departments or Affiliates the Supplier shall comply with the additional requirements included in the below table.

Control ID	Requirement	CCS	OMS
CT-90	The Cloud Services provider must host and storage SABIC´s information originated or owned by Saudi-Based departments or affiliates inside the Kingdom of Saudi Arabia.	✓	
CT-91	The Cloud Services provider must fulfill NCA's requests to remove software or services, provided by third-party providers that may be considered a cybersecurity threat to national organizations, from the marketplace provided to SABIC	✓	
CT-92	**If SABIC´s information originated or owned by Saudi-Based classified by SABIC as critical** is involved in the cloud service: The Cloud services provider must be following NCA's Cloud Cybersecurity Controls (CCC)	✓	
CT-93	**If SABIC data or systems classified by SABIC as critical** is involved in the service: Outsourcing services must rely on Saudi companies and organizations, in accordance with the relevant legislative and regulatory requirements.	✓	✓
CT-94	Cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia.	✓	✓
CT-95	**If a hosted telework system is provided to Saudi-Based SABIC systems,** it must be inside the Kingdom of Saudi Arabia.	✓	

8. REFERENCES

- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- National Cybersecurity Authority (Cloud Cybersecurity Controls (CCC) – 1: 2020)

9. APPENDIX A - CYBERSECURITY INCIDENT RESPONSE INSTRUCTIONS

The Supplier, in case of suffering any adverse situation or Cybersecurity incident in its environment, affecting any networks, systems or applications that process, access, or store SABIC's data, shall follow these basic instructions:.

Verify and identify :

- Supplier will verify received Incident alert and determine impact.
- If the incident affects any networks, systems or applications that process, access, or store SABIC's data, the Supplier must notify and report the incident to SABIC.
- The notification must be made as soon as practicable, but no later than twenty-four (24) hours.
- The Supplier must make the notification to SABIC using the following channel:
    - Email: CyberSecurityCenter@SABIC.COM
- Supplier can notify the incident additionally via a call through the following hotline number [+966556900971 OR +966133455080].
- SABIC will evaluate received notification and perform protection actions to protect SABIC, if required.
- SABIC will provide Supplier with details of protection action taken by SABIC.

Contain, Eradicate and Recover

- Supplier will build containment, eradication and recovery plan to mitigate incident.
- In case the incident is impacting SABIC data or services, the Supplier will provide plan progress report every 24 hours to SABIC/SOC.

Post-incident

- Supplier will provide final report to SABIC include RCA (root cause analysis) and remediation plan.
- SABIC will review and evaluate provided reports from third party to get back to normal operation.