GO Telecom

Third-Party Cybersecurity Standard

TrustNet Program

Table of Contents

About the TrustNet Program

The TrustNet program will require all the business partners engaging with GO Telecom to achieve TrustNet Certification. This certification process will be conducted through authorized audit firms, ensuring that these the business partners adhere to stringent cybersecurity norms and practices. The TrustNet Certification will act as a benchmark for cybersecurity compliance, enhancing overall security posture and trust in business relationships with the business partners.

The TrustNet Cybersecurity Standard (TNCS) for GO Telecom outlines essential cybersecurity requirements for its third-party partners. This standard aims to shield GO Telecom from potential cyber threats and elevate the security posture of its third-party partners. It establishes a foundational framework for ensuring robust cyber defenses in collaborative business engagements.

Business Partner Classification

The TrustNet Cybersecurity Standard (TNCS) for GO Telecom specifically applies to all the business partners engaged through contractual relationships. Detailed cybersecurity requirements vary based on the business partner's role and interaction with GO Telecom's infrastructure:

1. **Network Connectivity (NC):** For the business partners with network access to GO Telecom's corporate network, telecommunication network, including those using leased lines or VPN solutions.
2. **Outsourced Infrastructure (OI):** Covering the business partners managing, maintaining, or supporting computing infrastructure for GO Telecom.
3. **Critical Data Processor (CDP):** For those developing, accessing, or processing critical GO Telecom corporate data or GO Telecom customer’s data.
4. **Customized Software (CS):** Applicable to the business partners developing or hosting customized software or applications for GO Telecom.
5. **Cloud Service Provider (CSP):** Addressing the business partners providing cloud services (SaaS, PaaS, IaaS) for hosting, storing, or processing GO Telecom corporate data.

The TrustNet Cybersecurity Standard (TNCS) for GO Telecom is designed to safeguard assets and critical facilities accessed or managed by the business partners. It establishes necessary cybersecurity controls to ensure protection. Third parties are responsible for understanding and complying with these standards as they apply to their involvement with GO Telecom.

Deviation

If adherence to the TrustNet Cybersecurity Standard (TNCS) for GO Telecom is not technically feasible for the business partner, they are required to request a waiver. This process is for instances where full compliance cannot be achieved due to technical constraints.

Revisions

The TrustNet Cybersecurity Standard (TNCS) for GO Telecom will be reviewed and updated at least annually, or as necessary, by the GO Telecom Cybersecurity Department. This ensures the standard remains aligned with business needs. Significant updates or annual revisions to the standard will be communicated to the business partners engaged with GO Telecom.

Cybersecurity Controls Instructions

Under the TrustNet Cybersecurity Standard (TNCS) for GO Telecom:

- The Business Partners must adhere to the cybersecurity controls in Section (M) as a minimum requirement.
- If a The Business Partner's role involves multiple classifications due to their access to assets and facilities, they must also follow controls in Section (R), which are required to be considered based on the requirements.
- Compliance is based on The Business Partner's specific classification as communicated by GO Telecom.
- These controls are applicable across the data lifecycle and must be implemented on all systems and assets connecting to GO Telecom's network or handling GO Telecom data, ensuring security and authorized access.

Scope of TrustNetwork Cybersecurity Standard

The TrustNetwork Cybersecurity Standard by GO Telecom is applicable to all its business functions and projects that involve external services, as categorized by the GO Telecom procurement team. It requires that all Business Partners, consultants, third-party staff, onshore and offshore Business Partners who access or manage GO Telecom's information assets adhere to this standard.

The cybersecurity controls outlined in the TrustNetwork Standard must be implemented on all Business Partner systems and assets that interact with GO Telecom’s network or handle its data. These assets must be securely managed and made accessible only to authorized individuals on a need-to-know basis.

Document Owner

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

Business Partner Pre-qualification in TrustNet

- All Business Partners must undergo a technical prequalification and certification process (TrustNetwork Program) to meet GO Telecom's requirements.
- Business Partners are required to comply with the cybersecurity controls in this Standard for any access or privileges granted by GO Telecom to fulfill contractual obligations.
- Business Partners are given a 90-day grace period from contract award to fully implement these standards.
- In case of a Cybersecurity Incident, Business Partners must follow the Cybersecurity Incident Response guidelines in Section X, along with ongoing resolution efforts.
- Both existing and new Business Partners must sign the data processing and data protection agreements found in Section X.

Business Partner Cybersecurity Governance

- Business Partners must meet security requirements before accessing GO Telecom resources.
- Confidentiality of customer information must be maintained by all involved parties.
- Business Partners must have communication procedures for cybersecurity incidents.
- NDA signing is required for confidentiality of GO Telecom information.
- Policies to prevent unauthorized disclosure of GO Telecom's systems and data are necessary.
- Business Partners should align proposals and contracts with the requirements of this document.
- Security baseline provision for system components is essential.
- GO Telecom's software and internal information are not to be transferred without authorization.
- Secure systems approved by GO Telecom must be used for network access.
- GO Telecom reserves the right to audit connected systems and terminate connections if non-compliant.
- Upon contract termination, all GO Telecom assets and information must be returned.
- Data should not be stored on personal devices and secured file-sharing principles must be followed.
- Sanitization of data storage assets is required at contract end.
- Business Partners should consider encryption and data obfuscation to protect data.

Cybersecurity Risk Management

- In the context of cybersecurity risk management, Business Partners are responsible for identifying cyber risks relevant to their people, processes, and technologies. They are also accountable for informing the GO Telecom Cybersecurity Risk team promptly about these risks, including proposed mitigation actions and timelines. This accountability underscores the importance of proactive risk management and communication in maintaining robust cybersecurity practices.

Cybersecurity Requirements for Digital Assets

- Business Partners must have policies to prevent unauthorized use of their tools and sharing of sensitive information.
- Unused services or features should be disabled.

- Operating systems need to be configured for least privilege, allowing only necessary applications.
- Admin level account access should be restricted to essential personnel.
- Admin accounts are not for regular use and must be renamed.
- The built-in Guest account should be disabled unless needed.
- Review and secure configurations, including hardening and patching, are required before implementation.
- Only GO Telecom authorized software/tools are permitted, and any exceptions must be approved.

Cybersecurity Requirements for Identity Governance

Onboarding Prerequisites

- Business Partners must provide detailed information as per the profiling template.
- A single, qualified Security Manager should be identified as the point of contact for security matters.
- Regular security reporting and assurance of continuous compliance with GO Telecom's security requirements are mandatory.
- Contact details of the Security Manager and their supervisor must be provided.
- System component designs must adhere to GO Telecom's Cyber Security Architecture Requirements.
- NDAs are required for preserving confidentiality.
- Proposals and contracts must align with this document’s requirements.
- A Security baseline for all system components is necessary.
- Logical and physical infrastructure architecture designs in specified formats should be provided.
- Any external cybersecurity compliance requirements must be identified and documented.
- Cybersecurity incidents impacting GO Telecom or customers should be resolved, documented, and reported.
- Information on services/assets related to the partnership should be detailed as per the required template.

User Enrollment and De-enrollment

- Business Partner applications must ensure unique user and asset identification.
- Identifiers for users include email address, employee code/number, and names.
- For GO Telecom assets like workstations and servers, use Device ID, MAC address, IP address, and hostname.
- Users should have only one account per application.
- Business Partner applications must integrate with IDM solutions, providing user management APIs.
- These applications should expose user attributes, including last login time, for IDM integration.
- Secure protocols are required for application integrations.
- Business Partners must be able to create multiple accounts in their systems.

Authentication and Authorization

- Authentication is mandatory for all IT systems and applications.
- User authentication should verify identity using knowledge (passwords), possession (ID badge/key), or inherent traits (biometrics).
- Business Partner applications must choose appropriate authentication methods, including multi-factor authentication, based on risk.
- Secure authentication protocols are required, such as SAML, LDAPS, NTMLSSP etc.
- Re-authentication is necessary when authenticators, roles, security categories, or privileged functions change, or periodically.
- Multi-factor authentication is essential for critical systems and privileged accounts.
- Service account access should be securely managed, with interactive logins disabled.
- Access privileges should follow the least privilege principle.

Secure Login Parameters

- Authentication methods for system access must be secure and varied.
- Log-on procedures are designed to minimize unauthorized access.
- Secure log-in parameters include monitoring login attempts, masking passwords, locking accounts after multiple failed attempts, session timeouts, and encrypted authentication information.
- Multi-factor authentication and restricted connection times enhance security for critical systems.
- Exceptions to authentication mechanisms require strict approvals.
- Business Partners must integrate with GO Telecom's Identity and Access Management solutions.
- Documentation of all necessary accounts for system operation is required.
- Systems should not allow default or anonymous accounts and delete dormant user accounts.
- Business Partner applications must support specific integration protocols and access only through secure protocols.
- Network devices should integrate with Single Sign-On solutions where applicable.
- Secure Authentication: Business Partner applications must use robust authentication techniques, including multi-factor authentication and secure protocols like SAML and SSH. Logging in should disclose minimal system information, with strong identity verification methods preferred.
- Access Control: Access should be authenticated and based on the least privilege principle. User and system re-authentication is required for significant changes. Default, anonymous, or multiple application-level accounts are prohibited.
- System Integration and Management: Business Partner applications must integrate with GO Telecom's Identity and Access Management solutions and support protocols for secure integration. They should also manage user sessions securely, limit user privileges based on roles, and delete dormant accounts after a set period.

Privileged Account Management

- Privileged Utility Program Management: There should be an approved list of privileged utility programs and scripts for use within GO Telecom's environment. These programs must be securely stored and executed, with restricted access to a limited number of personnel.
- Administrator Privilege Limitation: Access to administrator and root privileges in GO Telecom's systems should be restricted to a limited number of users, emphasizing control and security of privileged accounts.

Password Management

- Password management systems must enforce initial password changes, periodic changes, and maintain a password history to prevent reuse.
- Passwords must be complex and validated for strength, with enforced changes at defined intervals for various account types.
- Scripting or hardcoded passwords are prohibited.
- Passwords should be stored and transmitted in encrypted forms.
- The partner-provided password management system should allow configurable settings including length, history, age, complexity, lockout durations, and thresholds.
- Two-factor authentication and password rotation capabilities are required.
- Passwords for partner applications must be encrypted and support API-based rotation and discovery of privileged accounts.

Cybersecurity Physical Access Requirements

- Business Partners must have a restricted area for staff accessing GO Telecom's network.
- Compliance with physical security policies is mandatory, including safeguarding sensitive information and materials.
- All GO Telecom information should remain on-site, be secured, and destroyed when no longer needed.

Cybersecurity Requirements for HR

Background Screening

- Business Partners must ensure thorough background checks for all staff involved in GO Telecom projects, covering employment history, education, residency, and law enforcement records.
- Screening reports should be shared with GO Telecom upon request.
- Data privacy regulations should be adhered to, with personal information masked in reports.
- GO Telecom ensures the retrieval or destruction of information assets at contract termination.
- Cybersecurity responsibilities and non-disclosure agreements must be included in contracts and remain valid post-employment.
- Business Partners are responsible for reporting policy violations and taking corrective actions, ensuring compliance with GO Telecom's cybersecurity policies and standards.

Cybersecurity Monitoring and Incident Response

- Business Partners must comply with formal incident response standards, promptly reporting potential incidents to GO Telecom.
- Unrelated cybersecurity incidents within the partner's organization must be disclosed if they could impact GO Telecom's reputation.
- Business Partners are required to detail their log management capabilities, including default settings.
- Log generation procedures must create detailed historical audits for at least one year.
- Access to sensitive logs, like root or admin, should be restricted and encrypted.
- System integration with GO Telecom's CSOC is essential.
- Regular review and protection against tampering of log facilities are mandatory.
- Logs must be retained and backed up for a minimum of 12 months.
- Alternatives must be provided if incompatibility with GO Telecom's SIEM/XDR solutions occurs.

Remote Access Requirements

- Business Partners must comply with GO Telecom's remote access policies, including multi-factor authentication and other controls.
- Prior consultation with the Cyber Security Team is required for setting up remote access.
- Insecure protocols like Telnet and FTP must be disabled.
- Clear ownership of remote access accounts is essential.
- Sharing of remote access credentials is strictly prohibited.
- Each staff or subcontractor must use a registered, GO Telecom-approved device for remote access, with Serial Number and MAC address registration for traceability. Non-compliance leads to accountability for breaches.

Approved Remote Access Methods

In the TrustNetwork Cybersecurity Standard by GO Telecom, the preferred methods for secure remote access are:

- Tunneling, SSL VPN, for secure communication channels without split tunneling.
- For B2B connections then site-to-site IPSEC VPN with restricted source IP and service ports whitelisting
- Portals offering centralized access to multiple applications with authentication.
- Direct application access with built-in security features.
- Remote system control from outside GO Telecom's internal network.

Business Partner TrustNet Cybersecurity Certification Program

In the TrustNetwork Cybersecurity Program for GO Telecom, partners are responsible for understanding and adhering to specific cybersecurity standards. Regular assessments are conducted to ensure compliance with these standards. Business Partners must follow detailed cybersecurity controls outlined in the program and refer to specific guidelines for implementation requirements. This ensures partners are fully aligned with GO Telecom's cybersecurity practices.

Section M – Minimum Cybersecurity Controls

The Business Partners must comply with all the **minimum** cybersecurity controls specified in this section.

REQUIREMENT TYPE	DOMAIN	SUB-DOMAIN	CONTROL ID	DESCRIPTION
General Requirements	IDENTIFY	Governance (GV)	TNC-M-1	The Business Partner must establish, maintain, and communicate Cybersecurity Policies and Standards. Such as The Business Partner must establish, maintain and communicate a Cybersecurity Acceptable Use Policy (AUP) governing the use of The Business Partner Technology Assets.
General Requirements	PROTECT	Access Control (AC)	TNC-M-2	All The Business Partner Technology Assets and Systems must be password protected. And Password protection measures must be enforced by The Business 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.
General Requirements	PROTECT	Access Control (AC)	TNC-M-3	Multi-factor authentication must be enforced on all remote access, including access from the Internet, to The Business Partner Company computing resources. Enforce on all access to Cloud services utilized by The Business Partner, including access to cloud-based email.
General Requirements	PROTECT	Access Control (AC)	TNC-M-4	The Business Partner must inform GO Telecom when employees provided with GO Telecom user credentials no longer need their access, or are transferred, re-assigned, retired, resigned or no longer associated with The Business Partner.
General Requirements	PROTECT	Awareness and Training (AT)	TNC-M-5	The Business Partner must inform personnel, in keeping with The Business Partner Company Policy, that using personal email to share and transmit GO Telecom data is strictly prohibited.
General Requirements	PROTECT	Data Security (DS)	TNC-M-6	The Business Partner must implement Sender Policy Framework (SPF) technology on the mail server. The Business Partner must enforce Sender Policy Framework (SPF) feature on GO Telecom email domain: go.com.sa The Business Partner must publish SPF record in DNS server.
General Requirements	PROTECT	Data Security (DS)	TNC-M-7	The Business Partner must inspect all incoming emails originating from the Internet using anti-spam protection.

REQUIREMENT TYPE	DOMAIN	SUB-DOMAIN	CONTROL ID	DESCRIPTION
General Requirements	PROTECT	Data Security (DS)	TNC-M-8	The Business Partner must use a private email domain. Generic domains, such as Gmail and Hotmail, must not be used.
General Requirements	PROTECT	Data Security (DS)	TNC-M-9	The Business Partner must implement a sanitization process before any Assets are loaned, destroyed, transferred, or repurposed. The assets that are used to process, or store GO Telecom data and information must be sanitized by the end of the Data Life Cycle, or by the end of the retention period as stated in the Contract, if defined. This includes all data copies such as backup copies created at any The Business Partner site(s). The sanitization must be conducted in alignment to industry best practices such as NIST 800-88. The Business Partner shall certify in a signed letter to GO Telecom that the data sanitization has been successfully completed.
General Requirements	PROTECT	Data Security (DS)	TNC-M-10	Firewalls must be configured and enabled on endpoint devices.
General Requirements	PROTECT	Data Security (DS)	TNC-M-11	If The Business Partner discovers a Cybersecurity Incident, The Business Partner must (besides its continuous efforts to resolve and mitigate the Incident): - Notify GO Telecom within twenty-four (24) hours of discovering the Incident - Follow the Cybersecurity Incident Response Instructions set forth in Appendix A and B.
General Requirements	PROTECT	Information Protection Processes and Procedures (IP)	TNC-M-12	The Business Partner must be staffed by employee(s) whose primary responsibility is Cybersecurity. The responsibilities of that personnel must include maintaining the business partner risks and security of information systems and ensuring compliance with existing policies.
General Requirements	PROTECT	Protective Technology (PT)	TNC-M-13	The Business Partner must conduct annual external Penetration Testing on its IT infrastructure systems, and internet facing applications.
General Requirements	RESPOND	Communications (CO)	TNC-M-14	The Business Partner must conduct annual external Penetration Testing on Cloud Computing Service(s) used by GO Telecom.

Section R – Required Cybersecurity Controls Based on Applicability

The Business Partners must comply with all the **required** cybersecurity controls specified in this section based on applicability.

REQUIREMENT TYPE	DOMAIN	SUB-DOMAIN	CONTROL ID	DESCRIPTION	NC	OI	CDP	CS	CSP
Specific Requirements	IDENTIFY	Governance (GV)	TNC-R-15	If The Business Partner is hosting a website for GO Telecom, annual Penetration Testing must be conducted to test website security.	✓	✓	✓	✓	✓
Specific Requirements	IDENTIFY	Governance (GV)	TNC-R-16	Third party data center must be certified by industry recognized authority	✓	✓			
Specific Requirements	IDENTIFY	Risk Assessment (RA)	TNC-R-17	The Business Partner must have a process to conduct Cybersecurity Risk Assessment on regular basis, to identify, assess and remediate Risks to data and information systems.	✓	✓		✓	✓
Specific Requirements	IDENTIFY	Risk Assessment (RA)	TNC-R-18	Users accessing applications and information systems must be issued unique user logins and passwords. Generic accounts must not be allowed, unless explicitly approved, restricted, and controlled. User access to the operating system, applications and database must be reviewed on a semiannual basis to determine if accessing personnel still require such access. All privileged accounts must be limited, justified, and reviewed on regular basis.					✓
Specific Requirements	IDENTIFY	Risk Assessment (RA)	TNC-R-19	The Business Partner must logically (e.g. partitioning a physical drive) and/or physically segregate data-at-rest related to GO Telecom from the data of other clients or customers.				✓	
Specific Requirements	IDENTIFY	Risk Assessment (RA)	TNC-R-20	GO Telecom Critical Data documents must only be shared with limited individuals who are part of the work specified in the Contract.					✓
Specific Requirements	IDENTIFY	Risk Management Strategy (RM)	TNC-R-21	Servers and workstations subnets must be segmented and access between them is restricted and monitored.	✓	✓			
Specific Requirements	PROTECT	Access Control (AC)	TNC-R-22	Servers accessible from the Internet must be placed in a DMZ (i.e. perimeter network) with restricted access to internal subnets.	✓	✓	✓	✓	✓

REQUIREMENT TYPE	DOMAIN	SUB-DOMAIN	CONTROL ID	DESCRIPTION	NC	OI	CDP	CS	CSP
Specific Requirements	PROTECT	Access Control (AC)	TNC-R-23	Wireless networks accessing information systems must use strong encryption for authentication and transmission, such as WPA2 or WPA2 Enterprise.	✓	✓	✓	✓	✓
Specific Requirements	PROTECT	Access Control (AC)	TNC-R-24	The Business Partner data center must have the required tier rating and high-availability of service failover as determined by GO Telecom			✓		
Specific Requirements	PROTECT	Access Control (AC)	TNC-R-25	Multi-Factor authentication must be enforced on GO Telecom users accessing Cloud Service Provider's Public Cloud Computing Service storing or hosting GO Telecom Critical Data.	✓	✓			
Specific Requirements	PROTECT	Access Control (AC)	TNC-R-26	Multi-Factor authentication must be enforced on end-users accessing Content Management Services (CMS) of Cloud Computing Service.	✓	✓	✓		
Specific Requirements	PROTECT	Access Control (AC)	TNC-R-27	The Business Partner must dedicate an access restricted working area for personnel with access to GO Telecom network.	✓	✓	✓	✓	✓
Specific Requirements	PROTECT	Access Control (AC)	TNC-R-28	Backup media must be secured to block/inhibit unauthorized physical access.					✓
Specific Requirements	PROTECT	Access Control (AC)	TNC-R-29	Technology Assets and Systems connected to the internet must be licensed and supported by the provider.					✓
Specific Requirements	PROTECT	Access Control (AC)	TNC-R-30	The Business Partner must encrypt data in transit (e.g. SSH, FTPS, HTTPS, TLS, IPSEC). The Business Partner must encrypt (e.g. using HTTPS) sessions where Critical GO Telecom information or data will be transmitted from and to the Public Cloud Computing Services, and enforce session authentication, lockout, and timeout.					✓
Specific Requirements	PROTECT	Access Control (AC)	TNC-R-31	The Business Partner must implement encryption mechanisms, using at least AES encryption algorithm, and 256-bit key, on all devices or storage media hosting sensitive data per the Business Partner’s assets classification policy.	✓				
Specific Requirements	PROTECT	Data Security (DS)	TNC-R-32	Encryption key management capability, including preservation and retrieval, must be defined, applied, and periodically reviewed.	✓	✓	✓	✓	✓

REQUIREMENT TYPE	DOMAIN	SUB-DOMAIN	CONTROL ID	DESCRIPTION	NC	OI	CDP	CS	CSP
Specific Requirements	PROTECT	Data Security (DS)	TNC-R-33	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.	✓	✓			
Specific Requirements	PROTECT	Data Security (DS)	TNC-R-34	Documents containing GO Telecom Critical Data, must be encrypted, and stored securely with access limited to authorized personnel.		✓	✓	✓	✓
Specific Requirements	PROTECT	Data Security (DS)	TNC-R-35	The Business Partner must implement data validation on all input fields for applications or Cloud Computing Services used by GO Telecom to only accept input with valid data type, syntax, and length range.					✓
Specific Requirements	PROTECT	Data Security (DS)	TNC-R-36	The Business Partner must create and manage baseline configurations to harden information systems. The hardening process must address configurations such as: • Resetting default usernames/passwords • Disabling unneeded software • Disabling unneeded services • Removing administrative access of users on workstations.	✓	✓	✓		✓
Specific Requirements	PROTECT	Data Security (DS)	TNC-R-37	The Business Partner must establish and follow regular procedures for backup of critical systems and GO Telecom's data, software, and websites. Backup stored at an off-site location must be encrypted using at least AES encryption algorithm, and 256 bits' key, except for data classified as public.					✓
Specific Requirements	PROTECT	Data Security (DS)	TNC-R-38	The Business 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.	✓	✓	✓		

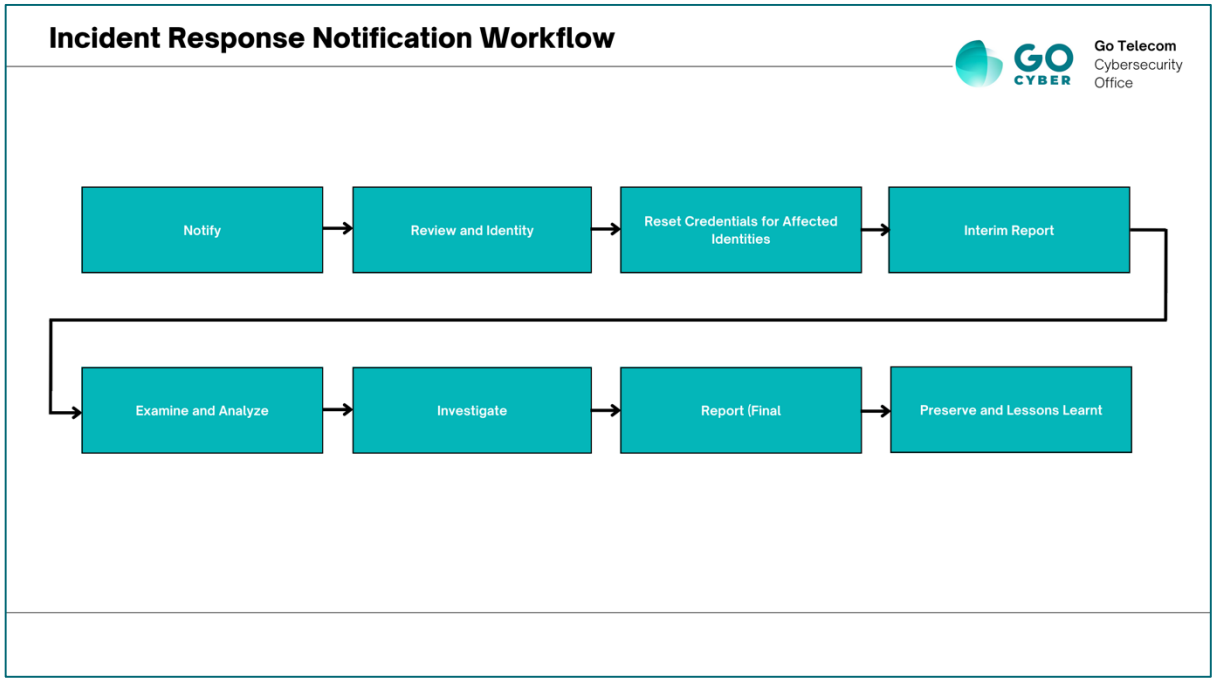
REQUIREMENT TYPE	DOMAIN	SUB-DOMAIN	CONTROL ID	DESCRIPTION	NC	OI	CDP	CS	CSP
Specific Requirements	PROTECT	Data Security (DS)	TNC-R-39	The Business Partner must have a comprehensive Business Continuity (BC) plan which is documented, maintained, and communicated to appropriate parties. The BC plan should 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. The Business Partner must conduct Business Continuity drills at least annually.			✓		
Specific Requirements	PROTECT	Data Security (DS)	TNC-R-40	The Business Partner must conduct security and source code vulnerability scanning on all developed applications, and close all discovered vulnerabilities before deployment in production.				✓	✓
Specific Requirements	PROTECT	Information Protection Processes and Procedures (IP)	TNC-R-41	All changes to the application must be properly authorized and tested in a testing environment before moving to production	✓	✓	✓	✓	✓
Specific Requirements	PROTECT	Information Protection Processes and Procedures (IP)	TNC-R-42	The Business Partner must have a process for secure system and software development life cycle in alignment with industry best practice.	✓	✓		✓	✓
Specific Requirements	PROTECT	Information Protection Processes and Procedures (IP)	TNC-R-43	The Business Partner must retain all audit logs from information systems and applications storing, processing or transmitting GO Telecom data for one (1) year.	✓	✓		✓	✓

REQUIREMENT TYPE	DOMAIN	SUB-DOMAIN	CONTROL ID	DESCRIPTION	NC	OI	CDP	CS	CSP
Specific Requirements	PROTECT	Information Protection Processes and Procedures (IP)	TNC-R-44	Firewalls must be implemented at the network perimeter and only required services must be allowed. Vulnerable services or insecure protocols should be blocked.	✓	✓		✓	✓
Specific Requirements	PROTECT	Information Protection Processes and Procedures (IP)	TNC-R-45	Network Intrusion Prevention Systems (IPS) must be implemented at the network perimeter. Signatures of firewalls, NIPS must be up-to-date.				✓	
Specific Requirements	PROTECT	Information Protection Processes and Procedures (IP)	TNC-R-46	If The Business Partner is hosting an application or a website for GO Telecom or providing cloud-based web application, Web Application Firewall (WAF) must be implemented to inspect all incoming traffic for potential threats and malicious activity e.g. SQL injection and Cross Site Scripting.				✓	
Specific Requirements	PROTECT	Information Protection Processes and Procedures (IP)	TNC-R-47	The Business Partner 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.				✓	✓
Specific Requirements	PROTECT	Protective Technology (PT)	TNC-R-48	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.	✓	✓		✓	✓
Specific Requirements	PROTECT	Protective Technology (PT)	TNC-R-49	Non-authorized devices (such as personal devices and mobile phones) must not be used to store, process or access Assets.	✓	✓	✓	✓	✓
Specific Requirements	PROTECT	Protective Technology (PT)	TNC-R-50	Monthly Vulnerability scans must be conducted to evaluate configuration, Patches and services for known Vulnerabilities.	✓	✓	✓	✓	✓
Specific Requirements	PROTECT	Protective Technology (PT)	TNC-R-51	Information systems and applications must log auditable events as stated in Appendix C.	✓	✓	✓	✓	✓

REQUIREMENT TYPE	DOMAIN	SUB-DOMAIN	CONTROL ID	DESCRIPTION	NC	OI	CDP	CS	CSP
Specific Requirements	PROTECT	Protective Technology (PT)	TNC-R-52	Incident management policy and plan must be documented, maintained and communicated to management and appropriate team members. The Business Partner 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.				✓	✓
Specific Requirements	DETECT	Anomalies and Events (AE)	TNC-R-53	The Business Partner must track, classify and document all Cybersecurity Incidents.	✓	✓		✓	✓
Specific Requirements	DETECT	Continuous Monitoring (CM)	TNC-R-54	The Business 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 fourteen (14) calendar days of critical vendor patch release, notification from GO Telecom, 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.	✓	✓	✓		
Specific Requirements	DETECT	Continuous Monitoring (CM)	TNC-R-55	If The Business Partner is hosting a website for GO Telecom or providing a Cloud Computing Service, the website / Cloud Computing Service must be secured by a Distributed Denial of Service (DDOS) protection.	✓	✓	✓		

Appendix A – Cybersecurity Incident Response Control

Cybersecurity Incident Response Instructions



Notify

- Initial Notification of Cybersecurity Incident: The Business Partner must notify GO Telecom Cybersecurity Department within 4-hours of discovering any Cybersecurity Incident.
- All notifications must be communicated to the cybersecurity department via the GO Telecom Security email: (cybersec@go.com.sa)
- Notify GO Telecom of the Cybersecurity Incident: After the Initial Notification of the Cybersecurity Incident, the Business Partner must notify GO Telecom of all Cybersecurity Incidents stemming from the initial Cybersecurity Incident via the communication method agreed by GO Telecom during the initial notification.

Review and Identify

- Immediately review all recent changes and modifications to information system users and access privileges for unauthorized modifications.
- Conduct a thorough review of the Partner's information systems for evidence of compromise.

Reset Credentials for Affected Identities

- Immediately change every password on information systems or identities that are compromised or suspected to be compromised due to the Cybersecurity Incident.
- Document containment actions in alignment with your Cybersecurity Team.

Report (Interim)

Provide GO Telecom with reports detailing the Cybersecurity Incident. The Business 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 for details of the report template.

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

Severity	Description
Low	Incidents with minimal impact on a small number of systems or individuals, negligible network disruption, and low risk of spread.
Medium	Incidents affecting a moderate number of systems or people, impacting non-critical systems, or a specific business unit.
High	Incidents posing significant risk across numerous systems or individuals, likely to cause substantial financial or legal repercussions, compromise data confidentiality, impact critical organizational systems, or have a high chance of widespread propagation and significant disruption.

Appendix B – Cybersecurity Incident Notification

Interim Report Template

The Business Partner is required to provide GO Telecom's cybersecurity team with a written status report on each Cybersecurity Incident within 24 hours of its discovery. Following the initial report, subsequent updates are to be given every 24 hours until the incident is resolved, using the specified report format provided by GO Telecom.

Business Partner Cyber Incident Interim Status Report	Report No.: #
Date:	MM/DD/YYYY
Business Partner Name:	
Business Partner ID:	
Business Partner Incident Coordinator Information	
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:	

Final Report

Business Report

A final business report on any Cybersecurity Incident is required within three business days post-resolution.

The report must include:

- Business Partner's name
- Incident Coordinator's contact details
- Cybersecurity Incident Coordinator for GO Telecom
- Incident date and time
- Classification based on TrustNetwork criteria
- Duration of the outage
- Incident's impact (e.g., reputational, operational)
- An executive summary of the incident

This final report ensures accountability and aids in future preventive measures.

Technical Report

Business Partners must submit a final report on cybersecurity incidents to the cybersecurity defense department within five business days of the incident’s resolution. The comprehensive report should include the Business Partner's details, incident classification, impact, and an overview. It should cover the incident's discovery, response, resources affected, and corrective actions taken. The conclusion should reflect on the incident's entirety and preventative measures implemented.

- Name of the Business Partner involved.
- Contact details for the Business Partner's designated incident response coordinator.
- Identification of GO Telecom's Cybersecurity Incident Coordinator.
- Timestamp of the incident's occurrence.
- Classification level of the incident as per TrustNetwork guidelines.
- Duration of any system outages and the overall impact scope.
- A high-level summary of the incident, including its effects on various aspects of the business.
- Detailed account of the incident, such as personnel involved, detection and reporting timeline, systems affected, incident magnitude, containment measures, root cause analysis, immediate corrective steps, and long-term preventative strategies.
    1. Roster of involved personnel and associated Business Partners who managed the Cybersecurity Incident.
    2. Detection timeline of the Cybersecurity Incident.
    3. Initial reporting details to GO Telecom regarding the Cybersecurity Incident.
    4. Enumeration of affected resources or services.
    5. Assessment of the Cybersecurity Incident's impact on GO Telecom, including scale and nature.
    6. Containment strategy employed for the Cybersecurity Incident.
    7. Analysis of the root cause of the disruption.
    8. Interim measures implemented to mitigate the Cybersecurity Incident.
    9. Long-term corrective actions established post-incident.

- Final thoughts summarizing the incident and its resolution.

Appendix C – Cybersecurity Audit and Event Logs

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)	
17	Network Traffic Anomalies	
18	Unauthorized Access Attempts	
19	Changes to Access Rights	
20	Security Software Health Checks	
21	Application Error Logs	
22	File Integrity Monitoring	
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	
11	Protocol used	
12	Application/service	
13	Data volume transferred	
14	Command or query	
15	Response time	
16	Geolocation of IP address	
17	System process ID	
18	Access mode (Read/Write/Delete)	
19	User agent	
20	Change before and after (for configuration changes)	
NO	**Event Type**	**Event Attributes**
1	Web Access/Error Logs	Admin Activity Audit Logs (Application)
	These events include changes to systems or applications, data changes (creation and destruction), and application installation and changes.	Data Access Audit Logs Application Event Audit Logs
2	Authentication, Authorization, and Access	Successful and failed authentications, authorizations, system access, data access, and application access.

3	Application Operation Logs	Operational logs detailing application performance and user interactions within the app.
4	Application Change Management Logs	Logs tracking updates, patches, and changes made to the application's codebase and configuration.

Appendix D – Securing Confidential Documents

To secure documents containing confidential information:

- Limit sharing to individuals named in the contract.
- Passwords for document access must not be stored or sent with the document.
- Communicate passwords separately, using a different method than the document delivery.
- Follow password protection protocols as per the specified control in the Standard.

Appendix E – Information Classification and Labeling

Business partners must align with the data classification standards outlined, which are integral to the NDMO Data Management and Personal Data Protection Standards.

This framework categorizes data based on severity levels from 'Public' up to 'Top Secret' classifications. These measures are crucial for safeguarding sensitive information and ensuring compliance with stringent data protection protocols.

Rate	Severity	Classification Level
1	None	Public
2	Low	Confidential
3	Medium	Secret
4	High	Top Secret

This table can be utilized by business partners to ensure compliance with the appropriate handling and protection levels for various data categories, as mandated by the NDMO Data Management and Personal Data Protection Standards for Business Partners classified as CDP – Critical Data Processor.

Appendix F – References

National Cybersecurity Authority – Essential Cybersecurity Controls ECC – 1:2018 NDMO
Data Management and Personal Data Protection Standards
NIST Cybersecurity Framework