GO

Telecom

Third-Party Cybersecurity Control Implementation Guideline

TrustNet Program

Disclaimer: The contents of this report should be treated by The Business Partners as CONFIDENTIAL and is intended solely for the use of the individual or entity to which it is addressed. This report may contain legally privileged information and may not be disclosed or forwarded to anyone else without authorization from GO Telecom.

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.

Cybersecurity Controls Requirement

The TrustNet Program aims to ensure all GO Telecom business partners meet cybersecurity mandates by acquiring TrustNet Certification through an approved auditor. This guide offers essential instructions for partners to comply with cybersecurity controls, facilitating the assembly of a complete evidence package for the certification process.

The TrustNet cybersecurity controls guidance is a key resource ensuring consistency in evidence submission for cybersecurity control compliance. It's applicable for remote assessments, requiring partners to submit a detailed assessment aligned with the document's criteria. For on-site assessments, auditors use the guideline to cross-check provided evidences. If a control is not applicable, partners must complete an inapplicability form, stating the reasons for each exemption.

Minimum Cybersecurity Controls

CONTROL ID	CONTROL STATEMENT	CONTROL REQUIREMENTS
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. 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.	• Develop and maintain up-to-date Cybersecurity Policies and Standards. • Ensure these documents are effectively communicated within the organization. • A written Cybersecurity Acceptable Use Policy (AUP) outlining the permissible uses of technology assets. • Documentation showing the policy has been disseminated and communicated to relevant personnel within the Business Partner's organization. • Acknowledgement forms or digital receipts confirming that the staff have read and agreed to the AUP. • Provide evidence for Waiver process. • Provide evidence for annual review
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. • Password must not be written down, electronically or authentication code. • The "Remember Passwords" feature must be disabled in web browsers.	• Ensure all technology assets and systems are secured with passwords. • Implement a policy mandating password protection for every piece of technology equipment. • Regularly audit and document compliance with this policy. • Password policy documents specifying requirements. • System configuration snapshots or reports confirming these settings. • Audit logs or system reports demonstrating enforcement and compliance with the policy. • User education materials on password management reflecting the policy guidelines.
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.	• Policy documents mandating the use of multi-factor authentication (MFA) for remote access. • Technical setup documents or screenshots showing MFA configurations. • Access management reports verifying MFA enforcement for remote connections. • Configuration settings or implementation guides showing MFA is enabled for cloud services and cloud-based email. • User access management policies that require MFA.

CONTROL ID	CONTROL STATEMENT	CONTROL REQUIREMENTS
TNC-M-4	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 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.	• Notify GO Telecom promptly when there are changes in the employment status of individuals with access to GO Telecom systems. • Regularly review and update the list of individuals with access. • Include a process in their internal off boarding procedures that ensures GO Telecom is informed of access revocation when necessary.
TNC-M-5	The Business Partner must inform personnel, in keeping with The Business Partner Company Policy, that using personal email or USB drives to share and transmit GO Telecom data is strictly prohibited. Similarly The Partner must inform personnel, in keeping with Partner Company Policy, that disclosing GO Telecom policies, procedures and standards or any type of data with unauthorized entities or on the Internet is strictly prohibited.	• Explicitly communicate through internal policies that the use of personal email for handling GO Telecom data is not allowed. • Document acknowledgment of this policy by personnel. • Incorporate this rule into the onboarding and regular cybersecurity training sessions.
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.	• Implement Sender Policy Framework (SPF) on their mail server. • Provide configuration records or screenshots as evidence of SPF implementation. • Enforce the Sender Policy Framework (SPF) feature on the GO Telecom email domain "go.com.sa." • Provide evidence of SPF enforcement, such as DNS records or email server configuration details. • Publish an SPF record in their DNS server for domain verification. • Provide evidence like DNS configuration snapshots or records to demonstrate the SPF record's presence.
TNC-M-7	The Business Partner must inspect all incoming emails originating from the Internet using anti-spam protection.	• Implement anti-spam protection measures for inspecting all incoming emails from the internet. • Provide configuration details or reports from their email system demonstrating active anti-spam filtering.

CONTROL ID	CONTROL STATEMENT	CONTROL REQUIREMENTS
TNC-M-8	The Business Partner must use a private email domain. Generic domains, such as Gmail and Hotmail, must not be used.	• Use a private, organization-specific email domain for all official communications. • Ensure that email addresses from generic domains like Gmail or Hotmail are not used for official purposes. • Provide policy documents or email system configurations as evidence of compliance with this requirement.
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.	• Documentation of the sanitization process, including procedures and steps to be followed. • Records of asset loan agreements or transfers indicating compliance with the sanitization process. • Evidence of asset destruction, transfer, or repurposing procedures, including sanitization steps. • Logs or reports from the sanitization process, showing the successful completion of sanitization. • Documentation of industry best practices for sanitization, referencing NIST 800-88. • Records of compliance with NIST 800-88 guidelines in the sanitization process. • Evidence of staff training and awareness regarding the sanitization process and NIST 800-88 guidelines. • Reports or logs showing regular reviews or audits of the sanitization process. • Sanitize all assets processing or storing GO Telecom data at the end of their data life cycle or contractual retention period. • This includes erasing all data copies, even backups, at any Business Partner location. • Follow industry best practices for data sanitization, like NIST 800-88 guidelines. • Provide a signed certification letter or a certification as an evidence to GO Telecom validating the process and confirming successful data sanitization.
TNC-M-10	Firewalls must be configured and enabled on endpoint devices.	• To meet this requirement, the Business Partner should ensure that firewalls are properly configured and activated on all endpoint devices.

CONTROL ID	CONTROL STATEMENT	CONTROL REQUIREMENTS
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.	• Notify GO Telecom within 24 hours of incident discovery. • Adhere to the Cybersecurity Incident Response Instructions as detailed in Appendix A and B of the GO Telecom Third Party Cybersecurity Standard

Requirement-Based Cybersecurity Controls

The following cybersecurity controls are based on The Business Partner classification as defined in the *Third-Party Cybersecurity Standard – TrustNet Program*.

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
TNC-R-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.	• Designated employee(s) whose primary role focuses on Cybersecurity (GRC and Defense). • Organizational charts or job descriptions evidencing these dedicated cybersecurity roles.
TNC-R-13	The Business Partner must conduct annual external Penetration Testing on its IT infrastructure systems, and internet facing applications.	• Conduct annual external Penetration Testing on their IT infrastructure and internet-facing applications. • Provide reports or certificates from these tests as evidence of compliance.
TNC-R-14	The Business Partner must conduct annual external Penetration Testing on Cloud Computing Service(s) used by GO Telecom.	• Conduct annual external Penetration Testing on their cloud infrastructure and internet-facing cloud services.
TNC-R-15	If The Business Partner is hosting a website for GO Telecom, annual Penetration Testing must be conducted to test website security.	• Perform annual Penetration Testing specifically for any websites hosted for GO Telecom. • Submit test results to confirm website security.
TNC-R-16	Third party data center must be certified by industry recognized authority	• The third-party data center used is certified by a recognized industry authority. • Relevant certification documents are available as proof of compliance.
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.	• Establish a regular process for conducting Cybersecurity Risk Assessments. • Identify, assess, and remediate risks to data and information systems. • Maintain records or reports of these assessments as evidence.

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
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.	• Issue unique logins and passwords for individual users. • Avoid using generic accounts, except under special approval and strict controls. • Review user access privileges to operating systems, applications, and databases every six months. • Verify the necessity of continued access for each user. • Limit the number of privileged accounts to only those personnel who require them for their roles. • Justify the need for privileged accounts, providing clear reasons for their existence. • Regularly review and assess the usage of privileged accounts to ensure they remain necessary and are not being misused.
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. 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. Physical access to the facility where information systems reside must be restricted and monitored.	• Implement logical or physical segregation methods to separate data-at-rest related to GO Telecom from the data of other clients or customers. • Ensure that data-at-rest related to GO Telecom is stored in isolated environments, either by using separate storage partitions or physical storage devices. • Implement access controls and permissions to restrict access to GO Telecom's data-at-rest only to authorized personnel. • Regularly review and audit the segregation measures to ensure they are effectively implemented and maintained. • Provide evidence of an inventory of critical facilities (e.g., data centers, network closets, operations centers, critical control centers). - Provide evidence of physical security monitoring controls are implemented and appropriate to detect potential cybersecurity events (e.g., sign in/out logs, motion detectors, security cameras, security lighting, security guards, door/window locks, automatic system lock when idle, restricted physical access to servers, workstations, network devices, network ports)

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
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.	• Restrict access to GO Telecom Critical Data documents to only those individuals who have a legitimate need to access them for the work specified in the Contract. • Implement access controls and permissions to ensure that only authorized personnel can view or edit Critical Data documents. • Maintain a record of individuals who have been granted access to Critical Data documents and regularly review and update this list to reflect changes in personnel assignments. • Ensure that individuals who no longer require access to Critical Data documents have their access revoked promptly. • Periodically review and audit access permissions to verify that they align with the work specified in the Contract and make adjustments as needed.
TNC-R-21	Servers and workstations subnets must be segmented and access between them is restricted and monitored.	• Implement network segmentation to create separate subnets for servers and workstations. • Configure access controls and firewall rules to restrict traffic between these subnets. • Monitor network traffic to detect and alert on any unauthorized attempts to access or communicate between these subnets. • Implement logging and auditing mechanisms to track network traffic between servers and workstations. • Regularly review and analyze network traffic logs to identify and investigate any anomalies or unauthorized access attempts. • Ensure that network segmentation and access restrictions are in place and functioning correctly to prevent unauthorized access between server and workstation subnets.
TNC-R-22	Servers accessible from the Internet must be placed in a DMZ (i.e. perimeter network) with restricted access to internal subnets.	• Identify servers that need to be accessible from the Internet. • Create a DMZ (Demilitarized Zone) or perimeter network to host these servers. • Implement network security measures to restrict access to the internal subnets from the DMZ.

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
		• Configure firewall rules and access controls to allow specific, necessary traffic between the DMZ and internal subnets. • Ensure that only authorized traffic is allowed between the DMZ and internal network segments. • Regularly review and update firewall rules and access controls to maintain the security of the DMZ. • Monitor network traffic to detect and alert on any unauthorized access attempts to servers in the DMZ. • Implement logging and auditing mechanisms to track and analyze traffic to and from servers in the DMZ. • Conduct periodic security assessments and penetration testing to identify and remediate vulnerabilities in the DMZ configuration. • Ensure that servers in the DMZ are hardened and securely configured to minimize security risks.
TNC-R-23	Wireless networks accessing information systems must use strong encryption for authentication and transmission, such as WPA2 or WPA2 Enterprise.	• Implement wireless networks that use strong encryption protocols, such as WPA2 (Wi-Fi Protected Access 2) or WPA2 Enterprise, for authentication and transmission. • Ensure that all wireless access points (APs) and devices connected to the network support WPA2 or WPA2 Enterprise. • Configure wireless networks to use WPA2 or WPA2 Enterprise as the encryption method. • Establish a secure authentication mechanism for users connecting to the wireless network, such as username and password (WPA2 Enterprise) or a strong pre-shared key (WPA2). • Regularly update and patch wireless devices and access points to address security vulnerabilities. • Monitor wireless network traffic for any unauthorized access attempts or suspicious activities. • Conduct periodic security assessments and penetration testing on the wireless network to identify and remediate vulnerabilities.

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
		• Implement access controls and restrictions to limit who can connect to the wireless network. • Enforce strong password policies for authentication to the wireless network. • Educate employees and users about the importance of secure wireless practices, including not sharing wireless passwords and avoiding public or unsecured Wi-Fi networks.
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	• Ensure that their data center meets the required tier rating as determined by GO Telecom (Tier 3). Tier ratings for data centers are defined by organizations like the Uptime Institute and represent different levels of availability and reliability. • Implement high-availability and failover mechanisms within the data center's infrastructure to minimize downtime and ensure uninterrupted service in case of hardware or network failures. • Regularly test and validate the failover capabilities to ensure they function as expected during a real outage or failure scenario. • Maintain documentation and records of the data center's tier rating certification and failover testing results for audit and compliance purposes.
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.	• Implement Multi-Factor Authentication (MFA) for GO Telecom users. • Apply MFA to access the Public Cloud Computing Service. • Protect critical GO Telecom data hosted in the cloud with MFA.
TNC-R-26	Multi-Factor authentication must be enforced on end-users accessing Content Management Services (CMS) of Cloud Computing Service.	• Enforce Multi-Factor Authentication (MFA) for end-users. • Apply MFA specifically to access Content Management Services (CMS). • Ensure security of CMS in Cloud Computing Service with MFA.
TNC-R-27	The Business Partner must dedicate an access restricted working area for personnel with access to GO Telecom network.	• Dedicate an access-restricted working area for personnel with GO Telecom network access.
TNC-R-28	Backup media must be secured to block/inhibit unauthorized physical access.	• Secure backup media to block/inhibit unauthorized physical access.

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
TNC-R-29	Technology Assets and Systems connected to the internet must be licensed and supported by the provider.	• Ensure that Technology Assets and Systems connected to the internet are licensed and supported by the provider.
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.	• Encrypt data in transit using protocols such as SSH, FTPS, HTTPS, TLS, and IPSEC. • Implementation of HTTPS for sessions transmitting Critical GO Telecom information. • Documentation of session authentication procedures. • Documentation of lockout and timeout policies for sessions. • Records of session encryption measures in place.
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.	• Documentation of encryption mechanisms used. • Records of AES encryption algorithm implementation. • Records of 256-bit key usage for encryption. • Documentation of devices and storage media where encryption is applied. • Compliance with the Business Partner's assets classification policy regarding encryption.
TNC-R-32	Encryption key management capability, including preservation and retrieval, must be defined, applied, and periodically reviewed.	• Documentation of the encryption key management capability, including policies and procedures. • Records of the implementation and application of encryption key management. • Documentation of periodic reviews and audits of encryption key management practices. • Any reports or findings from reviews or audits related to encryption key management.
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 • Not to use traffic anonymizers, proxies or sites redirectors when accessing GO services. .	• Documentation of the content-filtering technologies in use. • Configuration records showing the specific websites and services that are blocked. • Records of monitoring or audits to ensure the effectiveness of content filtering. • Reports or findings from reviews or audits related to content filtering.

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
		• Any incidents or breaches related to internet access that were detected or prevented by content filtering.
TNC-R-34	Documents containing GO Telecom Critical Data, must be encrypted, and stored securely with access limited to authorized personnel.	• Encryption records or logs for documents containing GO Telecom Critical Data. • Access control records indicating restricted access to authorized personnel. • Security policies or procedures related to the encryption and secure storage of critical data. • Audit or monitoring reports related to access control and encryption of critical data documents. • Incident reports or breach investigations related to critical data documents.
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.	• Documentation of data validation policies and procedures. • Source code reviews or code analysis reports showing the implementation of data validation in applications or cloud services. • Records of tests and validations conducted on input fields to ensure they accept valid data types, syntax, and length range. • Incident reports or security assessments related to data input validation issues, if any, and actions taken to address them.
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.	• Documentation of baseline configurations for information systems, including details on the configurations applied, such as resetting default usernames/passwords, disabling unneeded software and services, and removing administrative access of users on workstations. • Records of configuration changes and updates made to information systems. • Evidence of compliance checks or audits confirming the implementation of baseline configurations. • Reports or documentation of security assessments related to baseline configurations and any remediation actions taken. • Documentation of policies and procedures related to baseline configuration management.

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
		• Evidence of training or awareness programs for personnel involved in baseline configuration management.
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.	• Backup policies and procedures documentation outlining the process for regular backups. Including the use of AES encryption with a 256-bit key for off-site backups. • Backup schedules and plans indicating the frequency and timing of backups for critical systems and GO Telecom's data, software, and websites. • Records of backup processes and procedures. including the dates, times, and details of the data/software/websites and activities that are backed up. • Documentation of backup storage locations and methods for securing backups. • Evidence of backup testing and validation to ensure the integrity of backed-up data. • Evidence of compliance with encryption requirements for off-site backups based on data classification. • Reports or logs from backup systems or software showing successful backup operations, including successful encryption of off-site backups • Documentation of data retention policies for backed-up data. • Evidence of disaster recovery and business continuity plans that incorporate backup and data recovery processes. • Records of personnel responsible for backup operations and their training or qualifications. • Records of data classification decisions for specific data sets. • Evidence of regular reviews and audits of the backup procedures and practices. • Evidence of encryption key management practices for off-site backups. • Documentation of data classification policies, including the classification of data as public or non-public.

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
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.	• Documentation of the Disaster Recovery Plan (DR Plan), including all relevant details and procedures. • Records of regular maintenance and updates to the DR Plan. • Communication logs or notifications sent to appropriate parties regarding the DR Plan. • Testing and validation reports of the DR Plan, including results and any identified areas for improvement. • Documentation of the procedures to be followed for the recovery of Assets and communications. • Logs or reports of past incidents or disruptions and the application of the DR Plan. • Evidence of staff training and awareness regarding the DR Plan and its procedures. • Reports or logs showing regular reviews or audits of the DR Plan. • Evidence of certifications or validations of the DR Plan by recognized authorities if applicable.
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.	• Documentation of the Business Continuity (BC) plan, including details of scenarios and procedures. • Records of regular maintenance and updates to the BC plan. • Communication logs or notifications sent to appropriate parties regarding the BC plan. • Testing and validation reports of the BC plan, including results and any identified areas for improvement. • Documentation of the procedures to be followed for each scenario listed (a to i). • Logs or reports of past incidents or disruptions and the application of the BC plan. • Evidence of staff training and awareness regarding the BC plan and its procedures. • Reports or logs showing regular reviews or audits of the BC plan. • Evidence of certifications or validations of the BC plan by recognized authorities if applicable.

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
		• Records of annual Business Continuity drills, including dates, participants, and objectives. • Documentation of the scenarios or situations tested during each drill. • Reports or logs detailing the outcomes and results of each Business Continuity drill. • Any identified areas for improvement or lessons learned from the drills and actions taken to address them. • Documentation of communication to relevant stakeholders regarding the Business Continuity drills. • Training or awareness materials related to Business Continuity drills for participants. • Evidence of certifications or validations related to the Business Continuity drills if applicable. • Any documented changes or improvements made to the Business Continuity plan based on the results of the drills.
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.	• Records of security and source code vulnerability scanning conducted on developed applications. • Vulnerability scan reports detailing the vulnerabilities discovered. • Documentation of the actions taken to close or remediate the discovered vulnerabilities. • Evidence of testing and verification to ensure that vulnerabilities have been successfully closed. • Records of the date and time of vulnerability scanning. • Documentation of the scanning tools or services used for vulnerability assessment. • Any identified vulnerabilities that were not addressed and the reasons for not addressing them, if applicable. • Evidence of a review or approval process for deploying applications in production after vulnerability scanning. • Records of any changes or updates made to applications based on vulnerability scan findings. • Evidence of communication or coordination with development teams

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
		and stakeholders regarding vulnerability scanning and remediation. • Any improvements or changes made to the vulnerability scanning process based on feedback or audit findings.
TNC-R-41	All changes to the application must be properly authorized and tested in a testing environment before moving to production.	• Provide a simplified checklist to validate if third parties are meeting the TNC-R-73 compliance standard, which mandates that all application changes must be properly authorized and tested in a testing environment before moving to production: • **Authorization Verification**: Confirm that there is documented authorization for each application change. • **Testing Evidence**: Check for evidence of testing in a dedicated environment, including test results. • **Change Logs**: Review change management logs for detailed records of all application changes. • **Environment Equivalence**: Ensure the testing environment is equivalent to the production environment. • **Deployment Approval**: Verify that there is documented approval for deploying changes after successful testing.
TNC-R-42	The Business Partner must have a process for secure system and software development life cycle in alignment with industry best practice.	• **Provide Documentation of Development Process**: Evidence of a documented and structured development process. • **Provide Security Integration Records**: Proof of security practices integrated throughout the development life cycle.
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.	• **Provide Log Retention Policy**: Evidence of a policy mandating the retention of audit logs for at least one year. • **Provide Log Management Records**: Documentation showing the implementation of log management practices consistent with the retention policy.
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.	• **Provide Firewall Configuration Records**: Documentation of firewall configurations at the network perimeter, detailing allowed services. • **Provide Security Policy Documents**: Evidence of policies defining which

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
		services are considered required and secure. • **Provide Vulnerable Services Block List**: A list or records showing blocked vulnerable services and insecure protocols. • **Provide Network Diagrams**: Diagrams illustrating firewall placement at network perimeters. • **Provide Firewall Audit Reports**: Audit reports verifying that only required services are allowed and insecure protocols are blocked.
TNC-R-45	Network Intrusion Prevention Systems (IPS) must be implemented at the network perimeter. Signatures of firewalls, NIPS must be up-to-date.	• **Provide IPS Implementation Documentation**: Records or documents showing the implementation of IPS at the network perimeter. • **Provide Network Diagrams with IPS**: Diagrams indicating the placement and integration of IPS in the network infrastructure. • P**rovide IPS Configuration Records**: Details of the IPS configurations, ensuring they are appropriately set up at the network perimeter. • **Provide Update Records**: Documentation showing recent updates of firewall and NIPS signatures. • P**rovide Update Schedule**: A schedule or policy document detailing the frequency of signature updates.
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.	• **Provide WAF Implementation Documentation**: Records showing the implementation of WAF for relevant applications or websites. • **Provide Compliance Verification Evidence**: Audit or inspection reports confirming the presence and effective operation of the WAF in line with
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.	• **Provide Log Aggregation and Correlation System (SIEM) Documentation**: Records showing the system or platform used for aggregating and correlating data. • **Provide Regular Analysis Reports**: Copies of periodic reports generated from the aggregated and correlated data, highlighting key findings and insights.

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
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. The Business 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 Security badges must be issued to Partner employees. Personnel must wear picture identification badges always.	• **Provide Physical Security Policy Documentation**: Documentation of the physical security policies, including measures for access control. • **Provide Access Control System Records**: Records showing the implementation of authentication card key systems and door locks at entrances and exits. • **Provide Video Surveillance Documentation**: Evidence of video camera installation and monitoring at entrances and exits.
TNC-R-49	The Business Partner must install mobile device management solution with capability to Remote wipe solution on any Assets used to receive, store and/or produce Confidential information, or higher classification, for Go Telecom Non-authorized devices (such as personal devices and mobile phones) must not be used to store, process or access Assets.	• Provide evidence of ability to wipe data remotely on mobile devices when data are missing or stolen is enabled. • Provide evidence of policy related to remote access and remote wipe solution used • **Provide Device Use Policy Documentation**: Evidence of a policy that prohibits the use of non-authorized devices for storing, processing, or accessing assets. • **Provide Compliance Audit Reports**: Reports from audits or inspections verifying adherence to the policy against using non-authorized devices.
TNC-R-50	Monthly Vulnerability scans must be conducted to evaluate configuration, Patches and services for known Vulnerabilities.	• **Provide Vulnerability Scanning Schedule**: Documentation of the scheduled monthly vulnerability scanning plan. • **Provide Recent Scan Reports**: Copies of recent vulnerability scan reports, demonstrating the regular evaluation of configuration, patches, and services. • **Provide Remediation Records**: Records of any actions taken in response to vulnerabilities identified in the scans.
TNC-R-51	Information systems and applications must log auditable events as stated in Appendix C.	• **Provide Logging Standards Compliance Documentation**: Evidence showing compliance with the specific logging standards and requirements outlined in Appendix C.

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
		• **Provide Sample Log Files**: Examples of log files demonstrating the logging of auditable events as specified. • **Provide Logging Policy Documentation**: Documentation of policies governing the logging of auditable events in systems and applications. • **Provide Audit Compliance Reports**: Reports from audits or reviews confirming that logging practices are in line with the requirements of Appendix C.
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.	• **Provide Incident Management Policy Documentation**: Evidence of a written incident management policy and plan. • **Provide Incident Response Records**: Logs or reports of incident responses that demonstrate the application of the policy and plan in real situations. • **Provide Incident Response Plan Documentation**: Evidence of a comprehensive Incident Response Plan covering all required aspects. • **Provide Detection and Analysis Procedures**: Details of the procedures and tools used for incident detection and analysis. • **Provide Containment and Eradication Strategies**: Evidence of strategies and procedures for containment and eradication of incidents. • **Provide Recovery Procedures Documentation**: Documentation of recovery procedures post-incident. • **Provide Incident Logs and Lessons Learned**: Copies of incident logs and documentation of lessons learned from past incidents.
TNC-R-53	The Business Partner must track, classify and document all Cybersecurity Incidents.	• **Provide Sample Incident Reports**: Copies of sample incident reports demonstrating the tracking, classification, and documentation process. • **Provide Incident Log Summaries**: Summaries or logs showing the history of tracked and documented cybersecurity incidents.
TNC-R-54	The Business Partner must resolve or mitigate the identified security	• **Provide Vulnerability Management Policy**: Documentation of the policy

CONTROL ID	CONTROL STATEMENTS	CONTROL REQUIREMENTS
	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.	outlining the timeframes for resolving vulnerabilities based on their risk levels. • **Provide Critical Risk Resolution Records**: Records showing immediate correction or mitigation of critical risk vulnerabilities within 14 days of critical vendor patch release, notification from GO Telecom, or discovered security breach, whichever is earlier. • **Provide High Risk Resolution Records**: Evidence of resolving or mitigating high-risk vulnerabilities within one month of vendor patch release or discovered security breach, whichever is earlier. • **Provide Patch and Update Logs**: Logs or records of patches and updates applied to address these vulnerabilities. • **Provide Incident and Vulnerability Reports**: Reports or logs documenting the identification, classification, and resolution status of all relevant security vulnerabilities.
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.	• Provide DDoS Protection Implementation Documentation: Records or documents showing the implementation of DDoS protection for the website or cloud service. • Provide Service Agreements or Contracts: Copies of service agreements or contracts with DDoS protection providers, if applicable. • Provide Monitoring and Response Records: Evidence of monitoring for DDoS attacks and records of responses to any DDoS incidents.

Appendix A – References

National Cybersecurity Authority – Essential Cybersecurity Controls ECC – 1:2018
National Cybersecurity Authority – Essential Cybersecurity Controls ECC – Implementation Guideline
NDMO Data Management and Personal Data Protection Standards
NIST Cybersecurity Framework
GO Telecom – Third Party Cybersecurity Standard – TrustNet Program