txOne networks | Keep the Operation Running

Security Exhibit

Security Exhibit

As a global industrial cybersecurity leader, TXOne Networks recognises the importance of having robust information security practices. As a result, TXOne Networks maintains a company-wide information security program which adopts and enforces internal policies and procedures, designed to (a) satisfy security objectives, (b) identify reasonably foreseeable internal risks to security, and (c) minimize security risks.

1. Security Awareness, Employee Screening and Acceptable Use

All TXOne Networks employees and contractors undergo a security awareness training course upon hire and thereafter on a periodic basis. All employees and contractors are required to adhere to TXOne Networks Internet, Computer, Remote Access and Mobile device acceptable use policies. TXOne Networks has in place a formal disciplinary process for employees who have been found to be non-compliant with organizational information security policies. All new employees and contractors are required to agree to TXOne Networks' confidentiality and non-disclosure agreements.

2. Reporting & Security Certifications

TXOne Networks implements systems and processes designed to maintain and monitor compliance with its information security program. TXOne Networks has undertaken external validation of its security practices and holds ISO 27001 certification.

3. Asset Management

From procurement to disposal, TXOne Networks has implemented and maintained processes around asset identification, classification and management. This includes, ensuring adequate methods for access revocation, return and secure erasure of customer information as appropriate.

4. Access Control

TXOne Networks adheres to strong password management practices and multi-factor authentication. TXOne Networks implements appropriate Identity and Access Management capabilities which differentiate between regular and privileged account management. Access rights are provisioned in line with the least privilege principle. TXOne Networks manages all access and regularly reviews to ensure regular and privileged user access is upon termination of employment or change in duties. This shall include both physical and logical access.

5. Physical & Environmental Security

For all its physical locations, TXOne Networks utilises appropriate security barriers (e.g. card-controlled entry gates, manned reception desks and CCTV) to protect areas that contain information and information processing facilities. All such areas are protected and secured with appropriate entry mechanisms that only authorized personnel with appropriate access rights are able to access. Further, TXOne Networks operates a clear desk policy designed to protect the security of its information.

6. Network Security

TXOne Networks ensures that any assets used to store, transmit, or process information are protected by appropriate network controls and cyber security measures, including network access controls, network intrusion detection and prevention systems.

7. Security Log Review

Security logs are reviewed for all systems. Security event logs are also integrated with internal communication and alerting tools for real time oversight and event triage. If a security incident is suspected, it is reported to the TXOne Networks Infosec team, where a formal incident response plan is executed within an appropriate timeframe proportionate to the incident. In addition, InfoSec independently monitors TXOne Networks services environment logs.

8. Incident Response Plan

(a) If a security incident is discovered, the incident is prioritized based on severity. A dedicated team of technical experts is assigned to investigate, advise on containment procedures, perform forensics, and manage communication. Following an incident, the team examines the root cause, and revises the response plan accordingly.
(b) In the event of a breach involving personal data of a EU or EEA citizen, TXOne Networks will follow its obligations under GDPR. For more information, see: https://www.txone.com/privacy-policy.
(c) In the event of a breach involving personal data of residents in regions outside the European Union or European Economic Area, TXOne Networks will follow its obligations under applicable laws.
(d) Insofar as informing impacted customers is concerned, TXOne Networks shall inform any impacted parties after becoming aware of any security incident. A reasonable amount of detail about the likely impact on the customer of the security incident and the corrective actions taken or to be taken by TXOne Networks will be provided.
(e) TXOne Networks will cooperate with all impacted customers to provide any relevant information relating to the incident.

9. Vulnerability Assessment and Penetration Testing

TXOne Networks services undergo continuous security testing conducted by security experts. Before going live or implementing new features, the services must pass vulnerability scanning and penetration testing. When a vulnerability is detected, the system automatically notifies the account owners and the InfoSec team for appropriate remediation. The owners review the identified vulnerabilities and address them within a defined timeframe.

10. Business Continuity/Disaster Recovery

All services at TXOne Networks are underpinned by a tailored business continuity plan containing backup, recovery and testing plans. Such plans include defining and implementing standard procedures for varying situations and testing, updating, and reviewing such procedures. TXOne Networks conducts Business Impact Analysis (BIA) which assesses the impact of disruption to key information processing operations to determine the Maximum Tolerable Period of Disruption, Recovery Time Objective and Recovery Point Objective based on the assessment of the impact of disruption to key information processing operations.
TXOne Networks prepares business continuity plans based on the results of the BIA and performs a drill at least once a year. The business continuity plan is covered under our ISO 27001 certification. The ISO 27001 will be reviewed annually.
Copies of our Table of Content for the business continuity plan and the disaster recovery policy can be provided upon request. Access to the Table of Content will be subject to NDA.

11. Information Security in Development

TXOne Networks implements various controls throughout the software development lifecycle. These include the following:

a) Static Code Analysis
TXOne Nertworks' projects in active development are regularly scanned using a leading static analysis security tool. A clean scan is a requirement for each product release.
b) Dynamic Analysis of Web Applications
TXOne Networks InfoSec conducts web application assessments of all products and services which utilize web interfaces. The assessments are conducted for any major release and at least annually using several leading dynamic analysis scanners.
c) Software Composition Analysis
3rd Party Components included with TXOne Networks products and services are inventoried and monitored continuously against NVD vulnerability feeds. Vulnerabilities (CVEs) are prioritized according to the associated CVSS score.
d) Vulnerability and Patch Management
Vulnerabilities are continuously monitored and tracked via internal records. Each vulnerability is assigned a CVSS score. Patching requirements enforce timelines of addressing a vulnerability according to CVSS. In addition, vulnerabilities found and responsibly disclosed to TXOne Networks via external researchers are addressed and assigned CVEs as required through TXOne Networks' responsible disclosure program.
e) Safe Compilation
All C/C++ projects are scanned continuously to ensure flags for ASLR, PIE, SSP are enforced. Compliance and adoption of safe compile flags is monitored as part of the release criteria.
f) Secure Design Process

Engineers are required to review the application or service threat model for new features and significant product changes. Engineers must provide secure design documentation as part of the release criteria. Where appropriate, TXOne Networks leverages FIPS certified cryptography.

g) Change Control

TXOne Networks has a documented change management process that ensures all changes follow a validation and approval process through testing, staging and production system rollout. Changes are formally tracked and reviewed for complete traceability. All changes to code repositories are monitored and require detailed record, review and approval. TXOne Networks utilizes appropriate tools and processes for source control and change management.

12. Personal Data and Privacy

TXOne Networks has implemented a number of technical and organisational measures to ensure an appropriate level of security for personal data, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. To the extent that a customer's personal data is processed by TXOne Networks, those measures will be set out in a separate data processing agreement. More detailed information can be found at the following links:

https://www.txone.com/privacy-policy/
https://www.txone.com/data-collection-disclosure/

txOne networks

txone.com