INFORMATION SECURITY AND CYBERSECURITY POLICY

Doc. Number: IT-1

Original Effective Date: 12-31-2021

Last Revised Date: 03-1-2024

TERAWULF

Table of Contents

1. OVERVIEW

The purpose of cybersecurity is to ensure that information can be used when required in the conduct of business with the confidence that it is accurate and complete, and that it is adequately protected from misuse, unauthorized disclosure, damage or loss.

As a digital currency operating business, TeraWulf Inc. and its affiliates (collectively, “TeraWulf” or the “Company”) operate in an increasingly complex operating environment, managing cyber risk across organizational, technical and geographic boundaries. Threats can occur from a variety of points within the ecosystem in which TeraWulf operates.

This document provides an overview of the Company’s approach to information security and cybersecurity, and its practices to secure data, systems and data center operations.

TeraWulf’s cybersecurity strategy prioritizes detection, analysis and response to identify, anticipated or unexpected cyber threats, effective management of cyber risks, and resilience against cyber incidents.

A. PURPOSE

The purpose of this Information Security and Cybersecurity Policy (the “Cyber Policy”) is to define the policies and standards which must be applied to maintain the confidentiality, integrity and availability of the information and IT assets supporting the business processes of TeraWulf.

B. SCOPE

The Cyber Policy governs all aspects of hardware, software, communications equipment, networks and information (“IT Assets”), and applies to all TeraWulf employees, contractors (where applicable), , affiliates and others specifically authorized to access information and associated IT Assets owned, operated, controlled, or managed by the Company.

TeraWulf’s IT Assets may be owned, leased, hired, developed in house or purchased, and include all computing facilities along with the interconnecting networks. The Cyber Policy covers all assets and services which are operated, contracted and/or outsourced by the Company.

2. POLICIES AND PROCEDURES

A. GOVERNANCE AND OVERSIGHT

As a Nasdaq-listed company, TeraWulf manages the organization in a way that gives shareholders confidence that the Company is managing risks within our macro environment. In the case of cybersecurity risk, this includes the policies, procedures and processes that drive the Company's approach to cyber threats. The Cyber Policy identifies and documents threats, establishes information security mandates, evaluates compliance to these mandates, and detects and responds to security incidents.

The Company's VP of Information Technology, who also serves as the Company's Chief Information Security Officer ("CISO") is responsible for managing and implementing the Cyber Policy and reports directly to the Vice President of Operations. In addition, the VP of Information Technology sets Company-wide control requirements, assesses adherence to controls, identifies and prioritizes cybersecurity risks, and oversees incident protection and response.

The CISO reports at least annually to the Board of Directors ("Board"), or one of its committees, concerning the overall status of the Cyber Policy. The Cyber Policy is approved by the Company's Board. The Board takes an active interest in information security and cybersecurity matters and sets the Company's risk appetite in these areas, monitors progress, and receives regular updates.

A multifunctional cybersecurity committee comprised of Information Technology, Operations, Risk, and Finance meets quarterly to review the status of the Plan of Action and Milestones ("POAM") (document used to track vulnerabilities, including scan findings, penetration test findings, audit findings, policy weaknesses, etc., and actions to mitigate issues), discuss new vulnerabilities and threats, update risk assessments and propose changes and updates to the Cyber Policy.

Risk Assessments

TeraWulf recognizes the importance of effective risk management, particularly in relation to information security and cybersecurity. In the support of the Company's risk management framework, TeraWulf maintains a standardized Risk Management Program that identifies, quantifies and prioritizes risks. Accordingly, the Company performs a number of internal and external risk assessments to gauge the performance of the Cyber Policy. The purpose of these assessments is to accurately estimate the Company's risk profile and adhere to relevant regulatory requirements. Service providers and supply chain risk are evaluated prior to contract execution to reduce risk to TeraWulf. The Company expects to have its POAM documented in the first half of 2024.

The Company additionally conducts a variety of technical assessments, which will include penetration tests, and regularly reviews controls using both continuous monitoring and sample-based testing.

The results of internal and external risk assessments, together with control performance findings, are used to drive program initiatives and to identify and improve internal controls.

Policies and Standards

The Company maintains a comprehensive set of information security and cybersecurity policies and standards which take into consideration cybersecurity, data privacy laws and regulations that are applicable to the industry in which the Company operates.

Topics governed by the Cyber Policy include but are not limited to the following:

- Identity and access management
- Application and software security
- Infrastructure security
- Data security
- Cloud computing
- Technology operations
- Third party risk management

IT Asset Inventory

The Company maintains asset information for hardware in managed inventories throughout its lifecycle and such inventories are used to track each assets attributes, components, and operational status through demise.

Each IT Asset is assigned an owner. The Company has asset management for software and applications that include classifications based on their inherent risks.

TeraWulf has implemented controls designed to ensure secure data destruction at the end-of-life of a storage device.

Cyber Policy Updates

The Cyber Policy will be reviewed annually and updated as needed by the Company's CISO. Revisions will be kept about the changes made, and legacy policy documentation will be retained.

B. PREVENTION

Security Awareness and Training

The CISO maintains a cybersecurity training program, which is designed to help employees recognize information and cybersecurity concerns and respond accordingly. In particular, the training program is designed to provide all personnel with the knowledge and skills to prevent, identify, and escalate cybersecurity risks.

Cybersecurity training is required of all personnel (e.g., full-time and part-time employees). Training is provided to new hires shortly after their employment commencement date. Role-based training will be developed for those employees with privileged access to the network, physical security responsibilities, in leadership positions, and/or assigned to specialized roles such as incident response teams.

TeraWulf incorporates training themes based on regulatory guidance, industry best practices, and changes in the risk environment. TeraWulf ensures that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.

The Company's security awareness and training standards include but are not limited to the following:

a. Ensuring that organizational personnel are adequately trained to carry out their assigned information-security-related duties and responsibilities.
b. Ensuring that training is provided to ensure all parties within the scope of this Cyber Policy can recognize and report potential indicators of insider threat.
c. For the successful completion of security awareness training, employees must achieve passing test scores. The Information Technology group maintains a record of all personnel that have completed training.

d. Requiring all employees of TeraWulf who work as administrators or hold other positions with significant and relevant security operations responsibilities have adequate experience and training.
e. Security training is an ongoing process at TeraWulf. Personnel will be kept up to date on new improvements or threats to be mindful of.

Access Management

Password Controls

TeraWulf maintains defined password requirements documented in a formal standard outlined in the Technology Use Policy.

Multi-factor authentication (MFA) is required for any access to Company systems from outside the Company's network. Default contractor passwords will conform to the password policy set forth in the Technology Use Policy. Third-party contractors who require any system access sign the Contractor Network Access Form.

All Network Appliance/Application Service Account passwords for critical infrastructure are changed and conform to the strong password policy set forth in Technology Use Policy.

Remote Access for Personnel

Remote access from outside the Company's premises is enabled through a secure connection to a user's virtual private network (VPN) using MFA. TeraWulf's virtualized infrastructure is designed to provide the equivalent level of control as the Company's on-premises infrastructure, regardless of the geographical location it is accessed.

VPN access must be approved by the employee's supervisor and VPN accounts are allowed to access only data that is associated with the user's on-site role.

VPN access is allowed on corporate IT Assets only. The VPN client cannot be installed on employee-owned equipment.

Remote Access for Third Parties

From time to time, contractors may be granted VPN access so electronic assets can be administered remotely. External contractors are required to maintain on any computing asset connecting to the Company's network or comply with the following:

- Virus protection installed on devices.
- Minimum PC operating system requirements, as defined periodically by the Information Technology group.
- Firewall protection.
- Passwords for VPN access should never be saved with the VPN connection information allowing unauthorized access to Company network resources.
- Sensitive and/or critical Company documents shall not be saved or kept on vendor-owned equipment.

The Company retains the right to examine any device utilized for VPN access and can revoke privileges immediately.

Vendors are required to sign and return the Contractor Network Access Form prior to access being granted, and these requests are logged into the Help Desk with the VPN approval information.

Security Testing

The Company's Information Technology group conducts annual penetration tests to discover and evaluate the security of applications and infrastructure, focusing on high priority themes and risks.

The penetration testing methodology used by the Company combines manual and automated assessment techniques and the use of proprietary, commercial and open source assessment tools in a consistent and repeatable process. The methodologies typically cover the following activities:

- Pre-test preparation with asset owners
- Threat modeling and triaging
- Automatic dynamic / static scans and output verification of scans
- Vulnerability identification and confirmation testing
- Socialization of findings with asset owner
- Tracking and remediation of issues

- Retesting of remediated issues

Configuration Management

The Company employs configuration management to validate from a security perspective that the Company's systems continue to perform consistently and as expected over time.

Company systems are deployed using standard security practices, such as restricted file access permissions and logging.

Hard drives on company-provided laptops, which are only used for specific business purposes, are generally encrypted using industry standard tools.

An inactivity screen lock is enforced by a configuration policy on every endpoint.

Network Security

The Company's network environment is designed to emphasize security and resilience, including through the implementation of multiple network zones separated by firewalls and other controls.

Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS), such as feature sets in firewalls, are deployed at the network perimeter to monitor and block malicious activity.

Wireless access to the Company's infrastructure is only permitted from company-approved devices, for example company-issued laptops and registered employee devices such as smartphones.

System Monitoring and Vulnerability Management

The Company has a comprehensive vulnerability management program that includes frequent network-vulnerability scans of internal and external network environments. Vulnerabilities are resolved on a risk-adjusted basis, as required.

The Company has a process for known vulnerabilities. Each vulnerability is assigned a criticality rating based upon industry standard processes and aligned with a remediation plan. The timeframes for systems patching are documented. For cases where a vulnerability is identified and for which a patch is not yet available, the Company evaluates the adoption of appropriate compensating controls to minimize the likelihood of unauthorized access.

Data Protection

Data Loss Prevention (DLP) controls are designed and implemented to prevent content from leaving the Company that is not intended for external uses and distribution.

The Company maintains various surveillances to identify potential incidences of data exfiltration or insider threats, including using big data techniques.

Access to removable media, such as USB flash drives, writable CDs and local administrative and enhanced system functionality, is prohibited by default. When access to removable media is approved for specific business purposes, such access is strictly controlled and time-bound.

IT Staff oversees the Company's electronic communications monitoring and surveillance program, including the review of alerts potentially indicative of a variety of risks resulting in potential non-adherence to regulatory requirements and/or Company policy.

Encryption

The Company encrypts sensitive personal information in transit and at rest. Other types of data are encrypted and/or protected with compensating controls based upon regulatory, security and contractual considerations.

The Company uses strong industry standard encryption methods and the Information Technology group regularly reviews the strength of all encryption protocols.

Data Security

The Company ensures data security and privacy through mandatory controls and processes for all applications storing or processing personally identifiable information (PII), including end user computing tools. The program is continuously updated in accordance with applicable laws and regulations, and consistent with the Company's standards of business.

The Company urges a clean desk environment, instructing personnel to keep workspaces clear of paper containing sensitive data.

The Company has implemented controls which lock user workstations after a defined idle period. Personnel are advised to lock workstations when away from their desk.

The Company generally maintains controls to ensure secure data destruction at the end-of-life of a storage device. The Company has a process to identify end of life systems, prioritize upgrades or demise of the systems based on the criticality of supported devices.

Asset decommissioning is internally managed by the Information Technology group through workflow, inventory and scanning processes.

The Company retains records for various periods as needed to comply with applicable laws and regulations.

Physical Security

Physical security measures are deployed to protect the Company's data centers and offices. These measures may include card access, video surveillance, on-site security staff, environmental controls and visitor management.

Appropriate entry controls are implemented at secure access points to ensure only individuals with appropriate access levels are allowed access. These access points are monitored.

All visitors must have a confirmed host before being granted access to the Company's offices or data center facilities.

The Company's data centers' access is limited to essential support and operating personnel as well as other authorized visitors, contractors and personnel.

All facilities supporting Company business are protected from environmental hazards by the following controls, when applicable:

- Air conditioning units
- Fire detection systems
- Fire extinguishers
- Emergency lighting

Cloud Security

The Company has established controls for cloud applications including encryption and compensating controls, strict authentication, role-based access, centralized logging, network segmentation, and auditing.

Cloud hosted applications undergo a risk assessment and architecture review on a risk-adjusted basis that is performed by the Information Technology group. Each application is profiled to determine regulatory and risk-based requirements.

C. MONITORING AND DETECTION

Logging

TeraWulf has enabled logging for key events including failed logins, administrative activity, and change activity.

Logs are maintained in accordance with Company standards of one year and legal and regulatory requirements.

Security event logging is enabled to allow for system forensic analysis and surveillance analytics. Security event logs are protected from unauthorized access, modification and accidental or deliberate overwriting.

Malware Protection

Industry-standard anti-malware software is installed on Windows endpoints and servers and on the Company's email infrastructure.

Anti-malware alerts are monitored by the IT Staff. Malware is remediated and, if necessary, systems are rebuilt.

The Company subscribes to an email pre-filtering solution to reduce the amount of malware received by the Company's email gateway. TeraWulf also uses an email protection system that is designed to block spam, phishing and viruses from reaching personnel inboxes.

Monitoring tools are in place to notify appropriate personnel in the IT Staff of security issues. Alerts are classified, prioritized and actioned by appropriate personnel for timely remediation based on business criticality.

Security Monitoring and Intrusion Detection

TeraWulf's Information Technology group maintains a monitoring process to detect anomalous activity. The Company collects, analyzes, and correlates events data across the organization to perform real-time central aggregation to detect and prevent multifaceted cyber-attacks, leveraging a variety of sensors distributed across the Company's environment.

The Company authorizes and monitors any third-party connections and collects and retains relevant information. TeraWulf has certain automated alerts to identify and monitor any unauthorized access to a critical system by a third-party service provider.

Security Scans

TeraWulf's Information Technology group conducts quarterly external security scans of public servers and appliances to ensure sensitive and critical data are protected from threats. Scans are conducted using a security scanner software updated for current vulnerabilities. Vulnerability is assessed from these scans and actions taken when deemed necessary as a result of the scans. Any changes are documented.

Threat Intelligence

TeraWulf recognizes that cyber threat actors target the Company's networks, vendors, suppliers, and its personnel in order to conduct fraud, steal proprietary information, and/or disrupt the Company's ability to conduct business.

Security intelligence and threat information are regularly obtained from third-party intelligence service providers, industry consortia, internal monitoring, as well as public and governmental sources.

Cyber Insurance

The Company maintains a cybersecurity insurance policy that covers the Company's losses from a covered security incident. This policy also includes coverage for business interruption issues.

D. REMEDIATION

Please refer to the Company's Cybersecurity Incident Response Plan.

Business Continuity

The Company employs a business continuity and resilience framework to ensure it is prepared in the event of an operational disruption.

The Company's facilities have a defined mitigation strategy which identifies the criticality, recovery time objectives, dependence and recover strategies for core assets and processes.

Data Backup and Recovery

Data backups are written to an immutable, disk and tape based platforms for recovery purposes. Periodically, data is written to an encrypted tape media and stored for a period of one week.

The Company's record keeping, data backup and recovery processes are executed using an industry standard enterprise system. Processes are in place to identify, escalate, and remediate exceptions as appropriate.

User-driven recovery requests are streamlined through a ticketing system. Recovery attempts of backed up data are logged.

Technology Resilience

The Company has a technology resilience program to ensure internal applications and dependent infrastructure components demonstrate the appropriate level of resiliency and recovery based on business criticality.

The Company maintains a framework and recovery program to identify and mitigate cyber-destruction incidents like ransomware, including coordination among internal stakeholders and collaboration with external parties, such as law enforcement and regulators.