CATO NETWORKS

Service Organization Controls 3 Report

For the Period November 1, 2021 to October 31, 2022

REPORT ON CONTROLS PLACED IN OPERATION AT CATO NETWORKS LTD. RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY

Section I - Cato Networks Ltd.'s Management Assertion

February 14, 2023

We, as management of Cato Networks Ltd are responsible for:

- Identifying the Cato Networks Platform (System) and describing the boundaries of the System
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system.
- identifying, designing, implementing, operating, and monitoring effective controls over the Cato Networks Platform (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability and confidentiality set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Very truly yours,

Title
Signature

Section II – Independent Service Auditor

The Board of Directors
Cato Networks Ltd.

Scope
We have examined management's assertion, contained within the accompanying Management's Report of its Assertions on the Effectiveness of Its Controls over the Cato Networks Cloud Security Platform based on the Trust Services Criteria for Security, Availability and Confidentiality (Assertion), that Cato Networks Ltd.'s controls over Cato Networks Cloud Security Platform (System) were effective throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Cato Network's responsibilities
Cato Networks Ltd.'s management is responsible for its assertion, selecting the trust services categories and associated criteria on which the assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Cato Networks Cloud Security Platform (System) and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- identifying, designing, implementing, operating, and monitoring effective controls over the Cato Networks Cloud Security Platform (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement.

Service auditor's responsibilities
Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Cato Networks Ltd.'s relevant security, availability and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Cato Networks Ltd.'s cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations
Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Cato Networks Ltd.'s principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information

technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Cato Networks Ltd.'s controls over the system were effective throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria

Very truly yours,

Kost Forer Gabbay & Kasierer
A member of Ernst and Young Global Limited
February 14, 2023
Tel-Aviv Israel

Description of the Cato Networks Platform relevant to Security, Availability, and Confidentiality for the Period November 1, 2021 to October 31, 2022.

Company Overview and Background

Cato provides a SASE platform, converging SD-WAN, Zero Trust Network Access (ZTNA), network security, and Cloud Access Security Broker (CASB) into a global, cloud-native service. Cato optimizes and secures application access for all users and locations. Using Cato, customers easily migrate from MPLS to SD-WAN, optimize connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacenters and remote users into the network with a zero-trust architecture.

Products and Services

Cato Cloud connects all enterprise network resources, including branch locations, the mobile workforce, and physical and cloud datacenters, into a global and secure, cloud-native network service. With all WAN and Internet traffic consolidated in the cloud, Cato applies a suite of security services to protect all traffic at all times.

Cato Cloud is comprised of the following pillars:

- **Cato Global Private Backbone**: A global, geographically distributed, SLA-backed network of 70+ Pops, interconnected by multiple tier-1 carriers. The backbone's cloud-native software provides global routing optimization, self-healing capabilities, WAN optimization for maximum end-to-end throughput, and full encryption.

- **Cato Security as a Service:** A fully managed suite of enterprise-grade and agile network security capabilities, directly built into the Cato Global Private Backbone. Current services include a next-gen firewall/VPN, Secure Web Gateway, intrusion prevention, next-gen malware prevention, cloud security (CASB), remote access (ZTNA/SDP), and a Managed Threat Detection and Response (MDR) service.

- **Cato Edge SD-WAN ("Cato Socket"):** a WAN edge appliance that connects physical locations to Cato Cloud, and between edge devices, over any last mile transport (Internet, MPLS, 4G/LTE). The Cato Socket provides application-based policy-based routing and packet loss mitigation, driven by quality-of-service policies and provider link performance, packet loss, and jitter.

- **Cato Cloud and Mobility Solutions:** Cato easily and securely integrates cloud data centers and mobile users into the network. Cloud datacenters are securely connected via an agentless configuration, and mobile devices using a Cato Client for laptops, smartphones, and tablets, or clientless browser access options.

- **Cato Service Management:** Cato provides customers with a self-service management application for analytics and configuration. If applicable, Cato or its partners offer managed service options including site deployment, last-mile monitoring, and configuration of network and security policy changes.

Cato Cloud is seamlessly and continuously updated by Cato's dedicated networking and security experts, to ensure maximum service availability, optimal network performance, and the highest level of protection against emerging threats.

Overview of Company's Internal Control

A company's internal control is a process – affected by the entity's boards of directors, management, and other personnel – designed to enable the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations. The following section is a description of the five components of internal control for CATO Networks.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management, the Board of Directors, and others concerning the importance of controls and the emphasis given to controls in the entity's policies, procedures, methods, and organizational structure. Cato Networks' executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Policy and procedures documents for significant processes that address system requirements and relevant updates are available on the internal network.

Authority and Responsibility: Lines of authority and responsibility are clearly established throughout the organization and are communicated through Cato Networks':
(1) Management operating style,
(2) Organizational structure,
(3) Employee job descriptions, and
(4) Organizational policies and procedures

Board of Directors: The Company's board meets on a quarterly basis. The board meeting has a fix agenda. Meeting minutes are retained**.** The Board of Directors (BOD) of Cato Networks' is actively engaged in the governance of the Company and its strategic direction. Members of the Board meet to discuss matters pertinent to the Company and to review financial information.

Management Philosophy and Operating Style: The Management Team, chaired by the Chief Executive Officer ("CEO"), has been delegated by the Board the responsibility to manage Cato Networks and its business daily. Cato Networks is led by a team with proven ability in networking and cyber security. A management meeting is performed on a weekly basis in order to go through day-to-day issues**.** Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to Cato Network's employees within the Cato Networks internal portal**.** In its role, the Management Team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The Management Team designs policies and communications so that personnel understand Cato Networks' objectives, know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable.

Integrity and Ethical values: Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior are the products of Cato Networks' ethical and behavioral standards, how they are communicated and how they are monitored and enforced in its business activities.

Human Resources Policy and Practices: Human resource policies and practices relate to hiring, orienting, training, evaluating, promoting, and compensating personnel. The competence and integrity of Cato Networks' personnel are essential elements of its control environment. The organization's ability to recruit and retain highly trained, competent, and responsible personnel is dependent to a great extent on its human resource policies and practices.

Commitment to Competence*:* Competence at Cato Networks is designed to (1) identify and hire competent personnel, (2) provide employees with the training and information they need to perform their jobs, (3) evaluate the performance of employees to determine their ability to perform job assignments, and (4) through the performance evaluation process, identify opportunities for growth and job performance improvement. New professional employees that join Cato Networks are required to attend an On-Boarding welcome session which provides them with the necessary knowledge about the firm and general work procedures. Additionally, Cato Networks' Team Leaders are responsible for training plans for their newcomers. Professional training for existing employees is typically done only for new tools. An annual review for all employees takes place. Main review topics are: Job perception, performance feedback, and manager-employee open discussion. Currently this review is not based on quantitative objectives.

Control Activities

Control activities are the policies and procedures that enable management directives to be carried out to address risks to the achievement of the entity's objectives. Cato Networks' operating and functional units are required to implement control activities that help achieve business objectives associated with:

(1) The reliability of financial reporting,
(2) The effectiveness and efficiency of operations, and
(3) Compliance with applicable laws and regulations.

The controls activities are designed to address specific risks associated with Cato Networks operations and are reviewed as part of the risk assessment process. Cato Networks has developed formal policies and procedures covering various operational matters to document the requirements for performance of many control activities.

Risk Assessment

Risk identification: The process of identifying, assessing and managing risks is a critical component of Cato Networks's internal control system. The purpose of Cato Networks's risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. Risk analysis embodies identification of key business processes in which potential exposures of some consequence exist. Exposures defined by Cato Networks, considers both internal and external influences that may harm the entity's ability to provide reliable services.

Risk assessment: Ongoing monitoring and risks assessment procedures are built into the normal recurring activities of Cato Networks and include regular management and supervisory activities. Identified risks are analyzed through a process that includes estimating the potential significance of the risk. The assessment includes how the risk should be managed and whether to accept, avoid, reduce, or share the risk. A risk assessment meeting of the management team is performed annually, in order to assess the risks identified and resolution of risks process. The process is documented, maintained and all remediation activities must be approved by management. The Management Team considers the significance of the identified risks by determining the criticality and impact of the risks.

Risk Mitigation: Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the Company's.

Information and Communication

At Cato Networks, information is identified, captured, processed and reported by various information systems, as well as through conversations with clients, vendors, regulators and employees. Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties. Employees receive communications about their responsibilities and have the information necessary to carry out those responsibilities.

General Company Policies

Formal written policies for the principles and processes within the organization are developed and communicated so that personnel understand Cato Networks' objectives. The assigned policy owner updates the policy annually and the policy is reviewed and approved by designated members of management. In addition, responsibility, and accountability for developing and maintaining the policies are assigned to relevant teams and are reviewed and approved on an annual basis by the management team. Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to Cato Networks employees within the internal network

Logical and Physical Access

Cato Networks has established an organization-wide information security policy designed to protect information at a level commensurate with its value. The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission.

Access Control, User and Permissions Management

Cato Networks builds its production environment system architecture using the AWS services and other hosting providers. Firewall detailed configuration is defined and performed by the Cato Networks Operations team. In addition, the global management of the Cato Networks infrastructure is performed by Cato Networks using a dedicated AWS workspace. This interface allows Cato Networks to, among others, (1) add, modify, and manage servers, (2) create security policies as they relate to these servers, (3) configure network and firewall parameters, (4) manage the databases and (5) manage AWS users. Firewalls separate the internal network from the internet.

Cato Networks manages and delivers its services using a variety of systems and environments. As previously described, information security controls and procedures are implemented throughout these systems, to help prevent unauthorized access to data:

- Users are identified through the use of a user ID/password combination using the application and the database. Strong password configuration settings, where applicable, are enabled on the domain, application, and database. Including: (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of attempts to enter a password before the user ID is suspended, and (4) password complexity.
- The access to the Database is restricted to authorized personnel.
- Access to sensitive permissions within the build tool is restricted authorized personnel.
- Authorized access to the AWS hosting environment is performed from the Cato Networks network or using a VPN. The access within the production environment is performed using an MFA methodology.
- Administrative access to the Firewall management tool is restricted to authorized personnel.
- The database servers reside within the production environment. Access to the production environment servers is restricted to authorized personnel.
- Access to the customer environment web application interface is performed using personal production username and password for relevant users and MFA.

Recertification of Access Permissions

Cato Networks has implemented a recertification process to help ensure that only authorized personnel have access to the production interface, servers, environments, and databases. Employees are provided with the minimal access rights required to carry out their duties. A detailed ticket is opened in the ticketing system for new hire provisioning. This template includes all user detailed permissions. Permissions with the different environments (servers, database, and application) are reviewed and approved by the Cato Networks security team on a quarterly basis.

Revocation Process

Terminated employees who had access to the different Cato Network's environments have their permissions removed in a timely manner. Terminated employees complete a termination clearance process on their last day at Cato Networks, and the termination notification is documented and accessible within the Cato Networks ticketing system. This process includes revocation of access permissions to the systems and premises, as well as the return of the property, data and equipment.

Production Environment Logical Access

Admin access to the AWS servers is performed using a VPN between Cato Networks offices and the AWS Data Center. The access to the production server is performed using SSH key and is restricted to authorized personnel**.** Access to the production servers can only be performed from Cato Networks office or through VPN.

Access to the AWS management interface is restricted to authorized personnel. In addition, access to the production environment and databases is granted by the appropriate personnel, based on the employee role and documented. Access to the backup and offline storage is restricted to authorized individuals Additionally, strong password configuration settings, where applicable, are enabled on the domain, application and database.

Remote Access

Cato Networks' internal networks are protected using commercial firewalls configured and administered by the IT department. In addition, Cato Networks' production environment servers are protected by the AWS tools and controls configured by Cato Networks. Cato Networks employees are granted remote access to the internal production network environment based on the need-to-work principle. Remote access to the Production server is performed by using VPN clients and is restricted to authorized personnel.

Physical Access and Visitors

Cato Networks recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets, and restricted areas. Physical access to the Cato Networks office is restricted to authorized personnel using personal electronic identification cards. Visitors to the Cato Network's office are accompanied while on premises. Visitors register at the reception desk upon arrival by signing a visitor log.

Software Development Lifecycle (SDLC) Overview

The software development lifecycle consists of the following stages:

- Product/Engineering Requirements Definition
- Detailed Design
- Coding
- Testing
- General Availability (GA) Release

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the management team within the Change Management application. Change Management tickets are prioritized and labeled based on development phase and urgency. Changes are documented and prioritized using tickets within the change management application. The changes are connected to the source control in order to link the request to the actual code change**.** Each change goes through a life cycle. Permission to move the status of a work item is restricted to authorized personnel. Product requirements are constantly being collected from customers and from market research by Cato Networks Product Managers. These requirements combined with additional engineering improvement requirements are discussed by R&D managers and Product Managers and are converted to a Product

Requirements Document (PRD) that contains more specific description of required features and changes. The change request is reviewed and approved by management. Emergency changes are performed and updated as part of hot fixes, which follow the same process as described above though the timeframe may be shortened, and approvals may be provided after the change was already performed.

The R&D Managers review the PRD and provide a high-level effort estimation for every feature. The product managers work with the R&D managers to create a prioritized features list based on the effort estimation and required timeline of the release.

R&D Engineers are engaged with ongoing enhancements of the product functionality. R&D engineers check-in their respective code to a common source control system that provides extensive version tracking functionality and other software building abilities. All changes which are added to the Source Control contain information linking them to the relevant features and bugs. A "pull request" is opened within the source control management application that includes a code review and comments based on discussions between the developers. Administrative access to the source control is restricted to authorized personnel.

Software Testing and QA Process: Cato Networks Quality Assurance (QA) is constantly involved from early development stages. Based on the PRD, QA creates internal test plans. Test plans are reviewed by Product Managers and by R&D Team Leader responsible for the feature design. Cato Networks uses a set of automated testing in order to check the versions deployed to production. The tests include Unit, regression, and QA testing. Alerts are sent in case of test failure. A full QA cycle (Stabilization) includes regression and progression tests according to test plan documents. During this stage bugs are reported in the ticketing system. Manual tests are performed by the QA team. Each bug is assigned to an R&D Engineer for resolving with severity and a target version. Bugs that were targeted to the current version are fixed and verified as closed or are reopened.

Software Release: It is mandatory that all automation tests pass and that scans are free of Critical and High findings. Automation tests are performed using dedicated mechanisms on a regular basis in order to identify issues within the application. Cato Networks secured development process also includes an annual pen testing, whose findings are promptly fixed in following releases. Bugs or functional requests that are made by customers are reported in the ticketing system and marked with customer tag. Requests for functional enhancements are going to Product Managers backlog for future Releases.

Monitoring the Change Management Processes

A change management meeting is performed every week, to assess the risks identified and review changes required to the production environment. Action items are updated within as part of the process and change is approved only after review and assessment. In addition, metric reports are regularly issued to the Management Team in order to provide them with key indicators regarding the change management process.

Infrastructure Change Management Overview

Cato Networks regularly makes changes within its production environment in response to the evolving client and market needs. These changes include adding/removing/changing the configuration policies of existing servers or performing routine maintenance activities, software updates, and other infrastructure-related changes accordingly to available possibilities provides by the third-party vendors.

Description of the Production Environment

Production Environment

The processes described below are executed within Cato Networks' production environment, which is hosted in Amazon Web Services (AWS) and other hosting providers globally. The facilities comply with standards of quality, security, and reliability that enable Cato Networks to provide its services in an efficient and stable manner.

Network Infrastructure

Robust network infrastructure is essential for reliable and secure real-time data communication between the Cato Networks service components. To provide sufficient capacity, the Cato Networks network infrastructure relies on platforms provided by AWS and other hosting providers. To ensure appropriate network security levels, Cato Networks security standards and practices are backed by a multi-layered approach that incorporates practices for preventing security breaches, ensuring confidentiality, integrity, and availability. Cato Networks' security model encompasses the following components:

- Application layer security, including:
  - Various authentication schemas such as multi-factor authentication (MFA), unique ID and complex password policy
  - Logical security
  - Penetration testing
  - IP address source restriction
  - Customer data encryption at-rest and in transit
- Network and infrastructure security, including:
  - Network architecture
  - Risk management
  - AWS data centers
  - Cloud operation security (change management, monitoring, and log analysis)

Web, Application and Service Supporting Infrastructure Environment

Cato Networks utilizes multiple networking and cloud providers throughout the world, to create a global redundant and highly reliable backbone for customers' SD-WAN. The infrastructure is configured in a way that enables auto scaling capabilities. This allows supporting high performance during demand spikes to the services.

Production Monitoring

Cato Networks uses a suite of monitoring tools in order to monitor the service. Alerts are sent to relevant stakeholders based on pre-defined rules. The notifications are reviewed and processed according to their level of urgency**.** The notifications are reviewed and processed according to their level of urgency. Cato Networks' production network encompasses numerous components including web services, application and database servers, monitoring tools, and redundant network equipment provided as part of AWS and other hosting services. In addition, in order to improve service availability to clients and to support the operations of Cato Networks environments, Cato Networks maintains a dedicated Security team. The Security department is responsible for investigating escalated issues.

Security and Architecture

Cato Networks provides a secure, reliable, and resilient Service that has been designed from the ground up based on industry best practices. The below addresses the network and hardware infrastructure, software, and information security elements that Cato Networks delivers as part of this platform.

Data Center Security

Cato Networks relies on Amazon Web Services and other hosting providers' global infrastructure, including the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.). This infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards: FedRAMP, HIPAA, ISO 27001:2015, AICPA SOC 1, SOC 2, SOC 3 and PCI-DSS and more.

Infrastructure Security

- **End-to-End Network Isolation** - Virtual Private environments designed to be logically separated from other cloud customers and to prevent data within the cloud being intercepted.

- **External & Internal enforcement points** - All servers are protected by firewall rules. The configuration of firewall rules is restricted to authorized personnel.

- **Server Hardening** - all servers are hardened according to industry best practices.

- **Segregation Between Office and Production Networks** – there is a complete separation between the Cato Networks Corporate network and the Production network. Access to the production environment is granted to authorized personnel only, and traffic between the networks is sent over an encrypted tunnel.

Application Security

- **Penetration Testing -** A penetration test is performed on an annual basis and high issues are resolved in a timely manner through the SDLC process**.**

- **Vulnerability Management -** Vulnerability scans are performed to the production environment on a quarterly basis, using an external tool, in order to detect potential security breaches. Web application architecture and implementation follow OWASP guidelines. The application is regularly tested for common vulnerabilities (such as CSRF, XSS, SQL Injection).

- **Segregation of Customer Data -** Cato Networks employs a login system and authorization mechanism based on industry best practices. During each user request, a validation process is performed through encrypted identifiers to ensure that only authorized users gain access to the specific data. The process is validated by third-party security consultants on a yearly basis.

Operational Security

- **Configuration and Patch Management -** Cato Networks employs a centrally managed configuration management system, including infrastructure-as-code systems through which predefined configurations are enforced on its servers, as well as the desired patch levels of the various software components.

- **Security Incident Response Management** - Whenever a security incident of a physical or electronic nature is suspected or confirmed, Cato Networks' engineers are instructed to follow appropriate procedures. Security Incident Response Policy is documented, reviewed and approved on an annual basis by the management team and available to Cato Networks employees.

- **Antivirus** - An antivirus/malware solution is installed on employees' laptops and the Company's app in order to detect and prevent infection of unauthorized or malicious software. Antivirus reports are sent to relevant stakeholders on a regular basis.

- **Unified Endpoint Management** - Cato Networks use a dedicate tool that implemented an Agent on the company's endpoints in order to monitor and control the updates, data, content, and configuration of the asset.

Human Resource Security

- **Security Awareness Training** - Cato Network's employees are going through a Security Awareness training on at least an annual basis**.** Training is performed periodically in conformance to Cato Networks' information security policy.

- **Secure Coding Standards and Training** - Cato Networks' R&D team is regularly trained in secure coding practices.

Data Encryption

- **Data in Transit** - All traffic between the customer's endpoint and the Cato Networks platform is encrypted using TLS with only the most secure algorithms enabled. Encryption between Cato Networks' customers and the service, as well as between Cato Networks sites is enabled using an authenticated tunnel. Connections to the Cato Networks network and databases are obtained through a secured tunnel, only accessible from within the production network. Clients' sessions and interactions are encrypted using HTTPS. Internet traffic is encrypted using high class level certificates based on PKI infrastructure.

- **Data at rest** – Data at rest is encrypted at the storage level using AES256. Customer content stored at rest is encrypted, without any action required from the customer, using one or more encryption mechanisms.

Support

Cato Networks' customer support procedures are designed to handle and resolve issues and requests in a timely manner. These includes issues that are internally identified, or issues submitted by clients. Support is available via support hotline and customer support portal. A support portal is available in order to guide the customer as to the correct use of the service. Support meetings with the management are performed regularly, in order to report major open issues to the management.

Cato Networks opens a ticket when an issue is raised by a client or when an issue is proactively identified. Client issues are documented, resolved, and closed by managing tickets in the CRM applications. Tickets are classified to the level of urgency and importance.

Incident Management Process

The company has developed an Incident management Policy in order to respond to Security Incidents and Personal Data Breaches. A ticketing system is available to Cato Networks employees in order to report breaches in system security, availability, and confidentiality. New employees are trained in the use of this system at the beginning of their employment.

Availability Procedures

Cato Networks' production environment is fully managed as part of the AWS and other hosting providers and monitored by Cato Networks Operations team using various tools. The application level is fully managed by the Cato Networks. Cato Networks has implemented the operations management controls described below to manage and execute production operations.

Database Backup and Restoration

Cato Networks application database is fully backed up according to the backup policy. The logs are replicated every day . In case of failure, a notification is sent to the Operations team. The access to the backup and offline storage is restricted to authorized individuals.

A restore process is performed and documented on an annual basis. The backup data captured as part of backup procedure is restored automatically into a separate environment in order to determine the integrity of data and potential data recovery issues. A log of the restoring process is sent to management for review.

Disaster Recovery Plan (BCP)

Cato Networks has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of disaster. The DRP is tested on an annual basis.

Confidentiality Procedures

Customer confidentiality is key factor in Cato Networks. As such, Cato Networks has implemented security measures to ensure the confidentiality of its customer's sensitive personal information. The security measures aim to prevent unauthorized access, disclosure, alteration, or destruction of sensitive personal information. Customers' passwords and PII are encrypted within the application database according to the Cato Networks security policy and according to SSS algorithm (Shamir`s secret Sharing). Customers are restricted to their own web interface environment and do not have access to view data from other environments. Traffic between Cato Networks' customers and the service, and connection to the production environments are encrypted using respectively HTTPS and SSH protocols.