Ensono Cybersecurity Program

March 2019

Table of Contents

Ensono Cybersecurity Program Overview

Ensono recognizes that information, and the systems used to process, store and transmit that information are critical to the success of Ensono and our clients. It is Ensono's responsibility to ensure that it maintains the trust of clients, associates, and other third parties by having appropriate processes and technologies in place to manage, control and protect that information.

Ensono has adopted the ISO 27002:2013 standard as the framework for the Cybersecurity Program. The ISO 27002 standard is based on guidelines and principles for initiating, implementing, improving and maintaining information security management within an organization. The framework consists of specific guidelines for the development of organizational security standards and effective security management practices.

The ISO 27002 standard is organized into fourteen (14) Control Categories. The 14 categories and a summary of Ensono's associated Cybersecurity Program is outlined below.

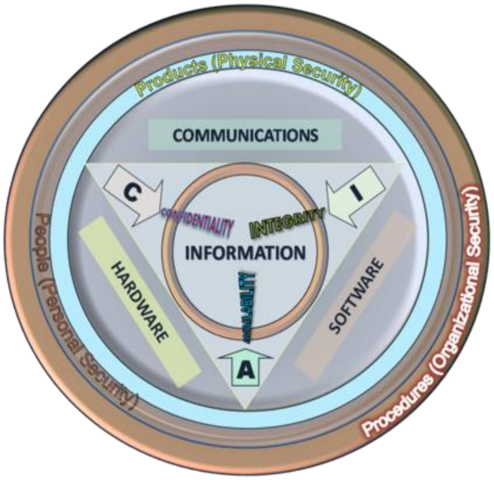
Ensono Information Security Policy

Ensono has a comprehensive and well-defined set of global policies. The objective of the policy framework is to protect Ensono and Ensono clients' assets and data and ensure compliance to applicable regulatory and privacy requirements for security.

The policy document is made available to Ensono associates, clients, vendors, contractors and other related business associates. Ensono associates may always access the document through a dedicated intranet site. The policy must also be read and acknowledged by all new associates, and by all employees on an annual basis.

Organizational Information Security

Executive Leadership: Ensono's Executive Leadership establishes accountability for Information Security and Enterprise Risk Management within the Ensono organization. Additionally, they maintain accountability to the Ensono Board of Directors for overall risk to the Ensono business.


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
HARDWARE
SOFTWARE
AVAILABILITY
A
People (Personal Security)
Procedures (Organizational Security)

Information Owners: Information Owners have the responsibility for controlling the production, development, maintenance, use, and security of information, systems, and solutions.

Information System Users: Associates who have been granted explicit authorization to access, modify, delete, and/or utilize information by the relevant Information Owner. Users must comply with all components of the information security program

Cybersecurity Team: Ensono's information security program is coordinated globally by the

Cybersecurity Team, led by the Global Sr. Director of Cyber Security and supported by the Security Risk Management and Operational Security Teams.

Segregation of Duties: Controls have been put in place to ensure that conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Ensono and client assets.

Mobile Devices: Ensono has deployed multiple controls such as encryption, malware protection, multi factor authentication and training to manage Ensono associate use of mobile devices.

Human Resources Security

Job Applicants: Ensono's policy is to screen all job applicants. Where local law allows, screening includes reference checks, examination of criminal conviction records, driver's license records, as well as verification of previous employment, education and professional qualifications.

All associates are required to sign a non-disclosure agreement as part of the terms and conditions of employment. These terms and conditions include the associate's security and legal responsibilities regarding the handling of information, the use of information processing facilities, and consequences of not complying with security or legal requirements.

Security Awareness Training: Ensono has established a security awareness training program that provides associates with an overview of information security best practices, specific laws and regulations that must be followed to ensure the confidentiality, integrity and availability of information.

The training also reviews compliance with Health Insurance Portability and Accountability Act, GDPR, PCI as well as Personally Identifiable Information protection. Additional specialized training (such as IRS Pub 1075) is provided as needed.

The Security Awareness program explains the importance of compliance and trains employees on expected behaviors, such as ethical conduct, acceptable and inappropriate usage of information.

Asset Management

Asset Acquisitions: Ensono has developed formal processes and procedures for acquiring assets. All large-scale projects require a formal business plan and proper technical and financial approvals before a contract can be signed.

All client production computer systems must be classified as such. The asset classification process considers the business process involved, the impact to the client, service level agreements, and any legal or regulatory requirements for data and the processing involved. The classification is also an integral part of system contingency planning.

Acceptable Use Of Assets: Ensono has established a formal Acceptable use Policy for Ensono and client assets. Use of information assets or facilities either owned, managed or leased, is limited to authorized users.

In all cases, Ensono associates are made aware that they are responsible for their use of assets and for any use carried out while under their responsibility.

Asset Implementation: Ensono has established a Project Management Office (PMO), which is responsible for managing all IT related projects. During the planning process, the resources needed for delivering Ensono and client work products are identified, a schedule to complete the work is produced, and commitments are negotiated. To track and provide oversight on a project effectively each project manager must compare actual progress against the plan, evaluate and assess the impact of any deviations from the plan, and determine corrective actions.

ASSET CHANGE MANAGEMENT: Ensono has established a formal change management process, which utilizes a standard methodology that can integrate with the client's change control requirements. The goal of the Ensono change management process is to minimize the impact of change-related events upon IT service quality through review, coordination and communication.

INFORMATION CLASSIFICATION: Ensono considers information to be an asset that has value to the organization and consequently needs to be suitably protected.

Ensono has created an Information Classification Policy that establishes the rules to determine what information can be disclosed, as well as the relative sensitivity of information that can or cannot be disclosed without proper authorization. Each classification level also specifies labeling and handling techniques to ensure information is appropriately protected.

Classification Level	Description
Public	Information that has been deemed appropriate for wide distribution. Disclosure is supported and often encouraged.
Internal Use Only	Information which cannot be considered Public due to the nature of the information, but is not of a sensitive nature that would harm Ensono or our clients should it be disclosed in an unauthorized manner (e.g. security standards, internal service offering documents, etc.) For this type of information, encryption is preferred but not required. Disclosure of INTERNAL USE ONLY information requires a Non-Disclosure Agreement to be on file.
Confidential	Information that is releasable to a limited number of associates and can be provided to a limited number of clients who have a legitimate business need, and with whom Ensono has a Non-Disclosure Agreement (NDA) on file. Its unauthorized disclosure could seriously and adversely impact Ensono, its associates, and/or clients. The Information Owner must define who is authorized to access CONFIDENTIAL information by job role and/or account team.
Restricted	Information that is specific to Ensono, Ensono associates, or Ensono clients and is regulated or private and sensitive in nature (e.g., Protected Health Information, Personally Identifiable Information, or Ensono financial data). Unauthorized disclosure could result in harm to an individual; legal action against Ensono; regulatory fines; or breach of contract. Access to this information must be strictly controlled, provided only on a need-to-know basis, encrypted in transit and at rest, and protected by the highest level of security controls available

Ensono Information Owners and business partners are expected to classify their information to ensure proper security is implemented and maintained.

Media Handling: Ensono has established policies and procedures for the handling and protection of electronic media throughout its life cycle. The policies and procedures include:

- Labeling of all media copies.
- The secure handling of removable media.
- The secure disposal of storage media.

The above procedures enable Ensono to ensure data is withheld from those who do not have authorized access to it and ensure we remain compliant with customer and legal requirements.

Access Control

Business Requirements and Associate Responsibilities: Ensono has established security policies, and procedures, based on business requirements, to ensure that access control is properly managed and information resources are properly protected. Ensono has established the following roles and responsibilities for everyone involved in the process:

- ***Information Owners:*** All Information Owners are responsible for:
    - Controlling the production, development, maintenance, use, and security of information, systems, and solutions.
    - Creating process and procedures that maintain compliance with Ensono's Information Security Policy.
    - Ensuring consistency between the access rights and information classification of the data they are responsible for.
    - Ensuring segregation of duties are maintained.
    - Ensuring access rights to information follow the principle of "Least Privilege".
- ***Information Users:*** All associates, using information or a system processing information are responsible for:
    - Conducting their day-to-day business practices in a way that supports the intent of Ensono's Information Security Policy
    - Understanding the information classification level of the information with which they are working.
    - Understanding the handling requirements for the classifications of information present at Ensono.
    - Notifying the Information Owner, their chain of management, or Cybersecurity in the event they feel a security incident has occurred.
    - Ensuring that authority to access information has been properly provided.
    - Complying with Ensono's security and privacy policies related to data handling.
    - Properly accessing, maintaining and securing the information which they access.

Access controls are clearly defined and are based on the following two principles:

Need to Know Principle – Associates must only be given access to information that they absolutely require to perform their job duties.

Default to No Access – Security mechanisms must default to no access, if nothing has been specifically configured for a user or the group of users

User Access Management: Logical access to all Ensono information systems and services is managed by a formal access control process. Each Ensono associate's access is determined by that associate's job responsibility. Also taken into consideration is the classification of information and segregation of duties requirements. Where it is applicable, vendor access is determined by the contracted services the vendor is to perform.

Ensono associate credentials consist of a unique login ID and password. Each password must comply with Ensono's policy regarding length and complexity. Credentials are also distributed in a secure manner and must never be shared. Password changes are required every 45 days.

Associate managers and Information Owners are responsible for reviewing access rights to systems and information on a quarterly basis. Accounts that are no longer necessary are disabled or deleted.

SYSTEM AND APPLICATION ACCESS CONTROL: Ensono has established security hardening standards for each operating system that exists within the environment. These standards are used by the system administrative teams to ensure the operating systems are secured utilizing a standardized configuration.

System owners are responsible for implementing and maintaining operating system security controls. These controls consist of identifying and verifying the identity, and access rights of each authenticated associate. Ensono's access control policy for authentication mandates that each Ensono associate use a unique credential that includes a strong password. Information assets that contain confidential and restricted data will be audited for successful and failed system access attempts.

Ensono's application owners are responsible for configuring security and granting access in accordance with Ensono's access control policy. Access must only be granted based on the associate's job function and with a business "need to know". All applications must be capable of controlling which data can be accessed by an associate and limit the access rights to read, write, delete or execute.

ACCESS CONTROL POLICY: Ensono's associates and third parties must have specific written approval from an authorized Ensono manager prior to being granted access to any computer or communication system resource.

PASSWORD MANAGEMENT: Each Ensono associate and third party is issued a unique credential that includes a complex password for access to Ensono system resources.

Where technically feasible, passwords are forced to change every 45 days, must be complex and be a minimum of 10 characters.

Associates are trained that all passwords must be treated as sensitive, confidential information. All users of Ensono systems are responsible for taking the appropriate action as outlined below to secure their passwords.

- Temporary or "first use" passwords must be changed the first time that the authorized user accesses the system.
- Do not share passwords with anyone
- Do not store passwords in un-encrypted form.
- Do not use the same password for company accounts as for other non-company accounts (e.g. personal email accounts).

ACCESS RIGHT REVIEW: Each Ensono manager must periodically review their associate's access rights and verify that they are correct.

CRYPTOGRAPHY

Ensono encrypts confidential data such as client information or authentication credentials while in transit over non-secure networks such as the Internet.

The Information Owner, in conjunction with Ensono Cybersecurity, is responsible for confirming that confidential data (including client data) is protected, where technically feasible, by implementing such technology as:

- One-way hashes (hashed indexes) such as SHA256
- Truncation or masking of sensitive data

- Strong cryptography, such as Triple-DES 128-bit or AES 256-bit, with associated key management processes and procedures
- Asymmetric public keys must use 2048-bit encryption.
- Commonly accepted cryptography in the form of RSA or an approved Public Key Infrastructure

Ensono does not allow the use of proprietary encryption algorithms. Only encryption technologies that have been approved by Ensono's Cybersecurity Team must be utilized.

Physical and Environmental Security

Physical Security Perimeter: Ensono defines the physical security for each of our facilities and implements the security controls for entry or exit points based on the identified risks. Where Ensono has deployed in third party facilities, we ensure that physical security controls meet our standards.

Secure areas are protected by access cards, monitoring and, where appropriate, based on risk, physical guards to ensure that only authorized personnel are allowed access. Associates working in higher secure areas, such as data centers, are subject to additional entry and monitoring controls that ensure an elevated level of security that further protects any sensitive information that is present. Delivery and loading areas are controlled and isolated from the information processing facilities to avoid unauthorized access.

Associates are required to wear their Ensono issued identification badges and are encouraged to challenge unescorted strangers and anyone not wearing visible identification. Ensono has a process developed to ensure badges are disabled and access rights removed when access is no longer required.

Visitors must be supervised or cleared and recorded before access is granted. Visitors are only granted access for specific, authorized purposes and are issued with instructions on the security requirements of the area and on emergency procedures.

Equipment Security: Ensono's physical security controls ensures that all information assets are physically protected from damage, theft, and other interruptions to business processes. Production systems, including servers, network equipment, network wire closets and voicemail systems, are all located within physically secured areas.

Security cameras are used to monitor physical access to areas with systems that store process or transmit sensitive data.

- Controls minimizing the risk of potential physical and environmental threats have been adopted.
- Guidelines that restrict eating and drinking in proximity to information processing facilities have also been adopted.

In addition to physical controls, each asset owner and facilities manager is responsible for protecting equipment from security threats. All servers are required to be in a securely controlled environment.

Equipment must be maintained according to the manufacture's specification to enable its continued availability and integrity.

Appropriate change control and safety processes must be observed for activities such as, but not limited to, lifting raised floor tiles, network cabling activity, modifying or adding electrical circuits, maintaining UPS and air conditioning systems, testing fire protection systems, and testing emergency alarm systems.

Operations Security

Change Management: Ensono has implemented a corporate change management program that provides a mechanism for controlling changes to the enterprise. The goal of the process is to minimize the impact of change-related activity through review, coordination, approvals and communication.

The program includes definitions for specific roles within the change management process to help ensure there is a segregation of duties within the approval process. The roles defined are structured to prevent a single person from controlling a change from beginning to end.

Ensono teams responsible for client-specific resources participate in client-specific change management meetings, and regular change meetings are held for shared environments with account team members to help ensure proper planning and communication with external clients.

A cross-divisional Change Management Team maintains documentation regarding the Ensono change management process. Events covered by the process include:

- Installation, removal, or relocation of computer hardware, environmental support equipment, data center systems software, operating systems software, local area network (LAN), data, voice network, and other systems hardware and software controlled or supported by Ensono
- Mass updates to shared infrastructure supported by Ensono
- Changes impacting production, test, and development infrastructures

The Change Type that is assigned to a change request, determines the process flow that will be followed for a change, and displays the planning details performed before a change is implemented.

There are three Change Types:

- Standard – Follows the Ensono recommended Lead Times.
- Emergency – The Lead Time is less than the standard amount required by the Change Management Support Process.
- Common – The change requests are preapproved templates. The change is well-defined and well-understood by the implementer with a low risk and low impact.

The change management process has been designed such that a user may rework a change order with updates. If after being reworked and the change order is still not approved, the approval task can be updated to Cancelled and the change order status marked as Cancelled.

Malware Protection: Ensono uses a combination of technologies from Symantec, Trend Micro and Sophos for malware protection. These technologies help ensure that managed devices have updated definition files, whether the devices are servers or workstations, which are always connected to the Ensono environment, or laptops which are rarely connected to an Ensono LAN.

All on-line systems will receive virus definition updates. This all happens without associate intervention.

Servers and workstations are configured to automatically download definition files as soon as they are available from the vendor. This mechanism includes systems that may not be attached to the Ensono network, typically remote laptop users or home office users. An Internet connection is all that is needed, and the client will silently download and apply virus definition updates.

Associates can also initiate a virus definition update session manually. By doing so, the client first attempts to download virus definition files from an update server located on Ensono's network. If the update server is not reachable, the client will download virus definition files directly from the vendor's secure update website.

Scanning Options: The centrally managed architecture allows administrators to configure scanning options on a single client, a group of clients, or every managed client using a single management console.

The default scanning options are set to scan all files as they are accessed or modified. The default scans cannot be disabled by unauthorized individuals. This ensures the virus-scanning feature will not be permanently disabled. A scheduled scan is configured, on each server and workstation, to run once each week at a pre-configured time set in the settings. Scheduled scans run against all files on local drives to ensure no known viruses or malware exist on the client. These scanning options are locked down preventing end-users from making changes and are set to provide maximum protection against viruses.

Associates are also provided with training material to recognize malicious software threats and are instructed on how to prevent computer viruses and report incidents.

BACKUP AND RECOVERY: Ensono has established standards for data backup, storage and recovery of applications and electronic information. The backup standards include; backup frequency, backup rotation scheme, backup verification, storage access and security, offsite storage and security, media labeling and maintenance.

The backup process is tested to verify that backed up information assets are recoverable. Restoration procedures are regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

Ensono's utilizes a shared backup environment which is monitored and provides reporting to facilitate tracking of any SLAs as well as any failures. Separate and distinct tape ranges are assigned to clients in order to segment client data. Data is written to the tapes using AES-256 hardware encryption and procedures are in place to securely dispose of media when no longer required.

CONTROL OF OPERATIONAL SOFTWARE: Ensono deploys a variety of different software tools to deliver and maintain its infrastructure and services. These tools are commercial off the shelf software that are vendor supported, configured, and implemented according to vendor specifications.

To minimize the risk of corruption to production systems, Ensono has established a standard process that is utilized before a production system is changed. The process includes testing, user acceptance, approvals and the creation of documentation. Only system administrators are authorized to request and perform changes to system files.

Ensono requires that each software development project must have identified individuals who are responsible for establishing and controlling the software baseline, which includes the following activities:

- Determining and acquiring all necessary source code and supporting software/products.
- Creating necessary code directories
- Determining security access levels for the project team
- Tracking all changes to software baseline throughout SDLC
- Migrating code to the test environment
- Ensuring that reviews and/or regression tests are performed to ensure that changes do not cause unintended effects to the software baseline

- Ensuring issues identified during testing are entered in a project issues log and are tracked to closure
- Conducting the software baseline audit.

Vulnerability Management: Ensono has a Vulnerability Management program which includes the categorization, prioritization, and remediation treatment procedures for identified vulnerabilities. The Program is comprised of Ensono's vulnerability scanning tools, Network-based Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), Malware Detection, and Security Information and Event Management (SIEM) solution. Ensono's Intrusion Detection System allows Ensono to quickly identify and handle suspicious network traffic and provides insights into threats and vulnerabilities. Ensono IP addresses within the Ensono perimeter, along with Ensono addresses accessible from the internet are scanned for vulnerabilities on a regular basis and Ensono engages a third-party to perform regular penetration testing.

Communications Security

Network Security Management: The Ensono network infrastructure is considered a critical asset to the organization. The network is comprised of a comprehensive suite of technologies that are critical to daily operations and communications. Therefore, Ensono has implemented layers of infrastructure and logical security as well as monitoring tools to protect the network.

Router configuration is restricted to the network engineering team, firewall configuration is restricted to the firewall engineering team. Passwords for all devices are periodically changed, stored, encrypted and transmitted across the network in a secure manner. Router and firewall authentication use a centrally managed solution with strong passwords and multi-factor authentication where necessary. Ensono's Network Operations Center (NOC) provides continuous network monitoring. Network logs for all critical Ensono devices are centrally managed using a Security Information and Event Management (SIEM) tool. Ensono network & security systems synchronize their clocks via NTP (Network Time Protocol), to help ensure consistent time stamps for logging and correlating events. All NTP distribution layers in Ensono are hierarchical, culminating at core centrally maintained servers, which themselves all synchronize directly back to NIST (National Institute of Standards and Technology) timeservers as their source.

Inbound Connections: Ensono does not allow access to the internal network directly from the internet. Encrypted connections must be established via Ensono's virtual private network (VPN) infrastructure. The VPN is TLS encrypted, and requires multi-factor authentication using a one-time pin as the second factor. When connecting via VPN, and before connecting to the internal Ensono network, associate devices are inspected to ensure current security controls are in place and that the device is an Ensono issued and managed device.

Ensono's Internet facing multi-user computer systems are deployed in Ensono managed demilitarized zones (DMZ). Access to Ensono's DMZs is protected by firewalls and an overall structure for multi-tiered security protections. Policies have been developed which govern access rules, firewall management, monitoring and auditing.

Associates accessing Ensono's internal network are presented with a login banner notice indicating that:

- Only authorized users may access the system.
- Users who login represent that they are authorized to do so.
- Unauthorized system usage or abuse is subject to disciplinary action including criminal prosecution
- System usage will be monitored and logged.

Outbound Connections: Ensono computer systems such as web servers, electronic commerce servers, and mail servers may not be attached to the Internet unless protected by multi-tiered firewall and IDS/IPS infrastructure. Logs from these devices are centrally monitored by Ensono's SIEM infrastructure.

Before Ensono associates connect their PC's to the Internet they must pass through Ensono's web filtering infrastructure. Filtering policies have been set to manage Ensono associate Internet usage.

Client Network Management: Ensono's company network is segmented from all client network environments. Each client network environment is segmented and dedicated per client, not only from Ensono but from other clients as well. Access to client networks by Ensono's client support teams is unique per each client's contracted requirements, regardless of whether computing resources are located physically in an Ensono data center, or remote at a client's site.

System Acquisition, Development and Maintenance

Ensono requires the integration of information security requirements into the software life cycle of information systems. The security requirements must identify controls that are needed to ensure confidentiality, integrity and availability. These controls must be appropriate, cost-effective and mitigate risks that may result from unauthorized access, use, disclosure, disruption, modification or destruction of the protected data.

System Development: Ensono requires that the business requirements definition phase of system development include a review of security requirements to ensure the system will comply with established security policies and standards.

Business requirements for new system development must include specifications for security controls. These specifications must address both automated controls and manual controls to be implemented. When implementing 'off the shelf' solutions, similar considerations must be part of the evaluation.

Application Development: While not core to Ensono's business, all application development is based on secure coding guidelines. Ensono's development teams follow the Open Web Application Security Project guidelines to introduce security best practices into their software development projects.

Supplier Relationships

Third parties who access Ensono information assets are required to adhere to Ensono information security policies and standards. Ensono has established a third-party risk management program to continuously identify and manage risks inherent in third-party relationships. As appropriate, a risk assessment is conducted to determine the specific implications and control requirements for the service being provided.

Supplier Access Control: Third-party service providers may be granted access to Ensono information assets only when they have a need for specific access in order to accomplish an authorized task. This access must be authorized by Ensono's Senior Management and based on the principles of business need and least privilege.

Any external parties, which are defined as trading partners, service providers, contractors, clients, customers, suppliers, vendors, outsource providers, and temporary employees, which are not part of the Ensono organization are controlled by setting limits on what can be seen, copied and modified.

When there is a requirement for a partner to access an Ensono information asset, a risk assessment must be carried out to determine security implications and control requirements.

Vendor support personnel are accompanied by Ensono Associate(s) while working in areas that house critical systems and have access to systems on a need-to-know basis.

Supplier Agreements: Supplier agreements are reviewed by multiple teams within Ensono to ensure that the right Information security, compliance and operational areas are covered. Additionally, responsibilities must be identified and agreed to.

Non-disclosure agreements are required for all business partners when confidential information is shared between the parties.

Information Security Incident Management

Ensono has implemented a formal Incident Response Program and Team to ensure that each incident within Ensono is managed and reported consistently throughout the enterprise. The Incident Response Team's remit is to manage all incident's whether they involve information security or not.

When an incident involves information security, Ensono's Cybersecurity Team is engaged. Ensono has developed a Security Incident Response Plan which compliments the broader Incident Response Program. The Security Incident Response Plan is designed to manage and minimize the impact of a security incident and ensure that the related tasks are executed in a uniform manner. Ensono follows a team approach when handling incidents. This enables individual team members to execute in parallel. The ability to operate in parallel reduces the overall response period.

All incidents are reported and tracked through a single point of contact. The information gathered is utilized to quickly contain the effects of the incident, manage resolution efforts, and measure the performance data that will continue to improve the incident handling response. Formal documentation regarding the "lessons learned" is published to heighten security awareness.

If a security incident were to impact client systems managed by Ensono, the client would be engaged as part of the incident response process, and the required notification terms.

Information Security Aspects of Business Continuity Management

Planning Information Security Continuity: Ensono has established a business continuity and disaster recovery management program. The program manages a continuity and recovery plan that is used to counteract interruptions to business activities and to protect critical business processes from the effect of major failures or disasters. The business continuity planning incorporates information security as part of the process to ensure continuity of security services as well as securing the overall business during a business interruption.

The consequences of disasters, security failures and loss of service are analyzed. Continuity plans are developed and implemented to ensure critical business processes can be restored within specific time frames based on specific business and customer requirements. Plans are maintained and practiced and are an integral part of all other management processes.

Business continuity management includes controls to identify and reduce risks limited to the consequences of damaging incidents and ensures the timely resumption of essential operations.

Implementing Information Security Continuity: The objective of the business continuation plan is to develop and document processes, procedures and actions that need to be taken to minimize the disruption impact on Ensono's product delivery and service commitments to its customers.

The business continuation planning establishes the processes and procedures to minimize the impact of unforeseen disruptive incidents on the delivery of service to customers. The objective is to effectively manage the disruption in an orderly manner through disaster recovery actions and return to normalcy at the earliest. Each business continuation plan includes processes, team structure, roles and responsibilities, tasks, communications, contact information, production asset capabilities, equipment and critical material supplier's information, capacity management strategies and alternatives.

Compliance

Compliance with Legal and Contractual Requirements: Ensono's Legal, Compliance and Information Security Teams monitor relevant statutory, regulatory, and contractual requirements and Ensono's approach to meeting these requirements. The specific controls and individual responsibilities to meet these requirements have been defined and documented.

Privacy and Protection of Personally Identifiable Information: Ensono has established a data protection & privacy program, which includes policy and process controls to safeguard personally identifiable information, and other regulated data. The policies and associated training are periodically communicated to all Ensono associates.

Additionally, Ensono has deployed the appropriate technical and organizational measures to protect personally identifiable information. The measures are tested on a periodic basis to ensure they are functioning as expected.

Independent Review of Information Security: Ensono initiates independent reviews on the suitability, adequacy and effectiveness of Ensono's approach to managing information security. Additionally, Ensono's clients also perform multiple reviews on the organization to ensure Ensono is meeting contractual and the applicable regulatory requirements. The reviews include assessing opportunities for improvement and any need for changes to the approach to security, including the policy and control objectives.