nisto

Nisto Security Plan

The Nisto Security Policy sets out the standards and guidelines for the secure use and handling of sensitive information within the Nisto Enterprise Web Application.

Aaron Lambie
President / CEO
Nisto

Revision: Oct 14, 2022.

1. INFORMATION SECURITY POLICY

Introduction

This Information Security Policy sets out the standards and guidelines for the secure use and handling of sensitive information within the Nisto Enterprise Web Application. The policy is designed to protect the confidentiality, integrity, and availability of sensitive information, and to ensure that Nisto complies with relevant legal and regulatory requirements.

Scope

This policy applies to all employees, contractors, and third-party service providers who use the Nisto Enterprise Web Application, as well as to all data processed by the application. The policy covers the use of the application, the handling of sensitive information, the management of user access, and the protection of data in storage and transit.

Confidentiality

Sensitive information must be protected against unauthorized access and disclosure. All employees, contractors, and third-party service providers must maintain the confidentiality of sensitive information, and must only use it for the purposes for which it was provided.

Integrity

Sensitive information must be protected against unauthorized modification. All employees, contractors, and third-party service providers must ensure that they use the Nisto Enterprise Web Application in a way that does not compromise the integrity of the information stored within it.

Availability

Sensitive information must be protected against unauthorized interference, disruption, or destruction. All employees, contractors, and third-party service providers must ensure that they use the Nisto Enterprise Web Application in a way that does not compromise the availability of the information stored within it.

User Access Management

Access to the Nisto Enterprise Web Application and the sensitive information stored within it must be controlled and monitored. Employees, contractors, and third-party service providers must only be granted access to the information that they need to perform their job functions. Access rights must be reviewed regularly and revoked when they are no longer needed.

Data Protection in Storage and Transit

Sensitive information must be protected against unauthorized access and modification both in storage and in transit. The Nisto Enterprise Web Application must be configured to use encryption to

protect the information in transit and must use appropriate security measures to protect the information in storage.

Incident Response

In the event of a security breach, the Nisto Enterprise Web Application has a well-defined incident response plan in place, to ensure that any security incidents are dealt with promptly and effectively. All employees, contractors, and third-party service providers must be trained to recognize and report security incidents and must be aware of their responsibilities under the incident response plan.

Compliance

All employees, contractors, and third-party service providers must comply with this Information Security Policy and any other security policies that apply to the use of the Nisto Enterprise Web Application. Non-compliance with this policy will result in disciplinary action, up to and including termination of employment or contract.

2. INCIDENT RESPONSE PLAN

Introduction

This Incident Response Plan sets out the procedures that will be followed in the event of a security breach or other incident affecting the Nisto Enterprise Web Application. The goal of the plan is to ensure that any incidents are dealt with promptly and effectively, to minimize the impact on the confidentiality, integrity, and availability of sensitive information, and to ensure that Nisto complies with relevant legal and regulatory requirements.

Scope

This plan applies to all incidents affecting the Nisto Enterprise Web Application, including security breaches, system failures, and natural disasters. The plan covers the initial response to an incident, the investigation of the incident, and the recovery from the incident.

Incident Response Team

The Incident Response Team (IRT) is responsible for responding to incidents affecting the Nisto Enterprise Web Application. The IRT will be comprised of representatives from relevant departments, including IT, Security, Legal, and Business Continuity. The IRT will be trained to respond to incidents and will be equipped with the tools and resources necessary to carry out their duties.

Current IRT includes: CEO, COO, VP of Software, and VP of Systems

Initial Response

In the event of an incident affecting the Nisto Enterprise Web Application, the following steps will be taken:

1. Notification: The incident must be reported to the IRT as soon as possible.
2. Containment: The IRT must take steps to contain the incident and prevent it from spreading.
3. Assessment: The IRT must assess the impact of the incident and determine the extent of the damage.
4. Notification of Authorities: The IRT must notify relevant authorities, as required by law or regulation.

Investigation

The IRT will investigate the incident to determine the cause and extent of the damage. The investigation may include the following steps:

1. Collection of Evidence: The IRT must collect evidence related to the incident, including system logs, network traffic, and other relevant data.
2. Analysis: The IRT must analyze the evidence to determine the cause of the incident and the extent of the damage.
3. Identification of Vulnerabilities: The IRT must identify any vulnerabilities that contributed to the incident and take steps to address them.

Recovery

The IRT will work to recover from the incident as quickly as possible while ensuring that sensitive information is protected. The recovery process may include the following steps:

1. Restoration of Services: The IRT must restore services as quickly as possible while ensuring that the restored services are secure.
2. Data Recovery: The IRT must recover any lost or damaged data, and ensure that it is protected.
3. Communication: The IRT must communicate with stakeholders, including employees, customers, and partners, to keep them informed about the status of the recovery process.

4. Lessons Learned: The IRT must conduct lessons learned review to identify areas for improvement and to ensure that the incident response process is as effective as possible.

3. ACCESS CONTROL PLAN

Introduction

This Access Control Plan outlines the procedures and policies that are used to control access to the Nisto Enterprise Web Application. The goal of the plan is to ensure that sensitive information is protected while ensuring that authorized users have access to the information they need to perform their jobs.

Scope

This plan applies to all users who access the Nisto Enterprise Web Application, including employees, contractors, and partners. The plan covers the process of granting and revoking access to the application, as well as the procedures for managing passwords and other authentication methods.

Access Control Policy

The following policies will be used to control access to the Nisto Enterprise Web Application:

1. Least Privilege: Users will be granted the minimum level of access necessary to perform their jobs.

2. Separation of Duties: Access to sensitive information will be restricted to multiple users, to minimize the risk of unauthorized access.

3. Role-Based Access Control: Access to the Nisto Enterprise Web Application will be based on the user's role within the organization.

4. Two-Factor Authentication: All users will be required to use two-factor authentication to access the application, to minimize the risk of unauthorized access.

Access Management Process

The following steps will be taken to manage access to the Nisto Enterprise Web Application:

1. Access Requests: Access to the Nisto Enterprise Web Application will be granted based on a formal access request, submitted by the user's manager or supervisor.

2. Approval Process: The access request will be reviewed and approved by the IT security team, who will ensure that the user has a valid business need for access to the application.

3. Provisioning: Once the access request has been approved, the user will be granted access to the application, based on their role within the organization.

4. Review: Access to the Nisto Enterprise Web Application will be reviewed on a regular basis, to ensure that users continue to have a valid business need for access.

5. Revocation: Access to the Nisto Enterprise Web Application will be revoked when a user no longer has a valid business need for access, or when a user leaves the organization.

Password Management

The following policies and procedures will be used to manage passwords for the Nisto Enterprise Web Application:

1. Password Complexity: Passwords must be complex, with a minimum length of 8 characters, and must include a combination of upper and lower case letters, numbers, and symbols.

2. Password Histories: Passwords will be stored in a secure, encrypted format, and a history of previous passwords will be maintained, to prevent users from reusing old passwords.

4. DATA BACKUP AND RECOVERY PLAN

Introduction

This Data Backup and Recovery Plan outlines the procedures and policies that will be used to ensure the integrity and availability of the data stored in the Nisto Enterprise Web Application. The goal of the plan is to minimize data loss in the event of a disaster and to ensure that data is available for recovery in a timely manner.

Scope

This plan applies to all data stored in the Nisto Enterprise Web Application, including user data, configuration data, and system data. The plan covers the process of backing up data, and the procedures for restoring data in the event of a disaster.

Backup Policy

The following policies will be followed to maintain the integrity of the data stored in the Nisto Enterprise Web Application:

1. Frequency: Data will be backed up daily to ensure that it is always recoverable.

2. Offsite Backup: To minimize the risk of data loss, backups will be stored in other data centers across the cloud.

3. Encryption: Backups will be encrypted to protect the confidentiality and privacy of the data.

4. Verification: Regular verification of backups will be done to confirm their completeness and usability.

Backup Process

The following steps will be followed to backup the data stored in the Nisto Enterprise Web Application:

1. Data Collection: The data, including user data, configuration data, and system data, will be collected from the Nisto Enterprise Web Application.

2. Compression: The collected data will be compressed to reduce the storage space required for backups.

3. Encryption: The compressed data will be encrypted to ensure the confidentiality and privacy of the data.

4. Storage: The encrypted data will be stored in secure locations across the cloud to minimize the risk of data loss in case of a disaster.

Recovery Process

The following steps will be taken to recover data in the event of a disaster:

1. Data Restore: The most recent backup will be used to restore the data, ensuring that it is available as soon as possible.

2. Verification: The restored data will be verified to confirm its completeness and usability.

3. Testing: The functionality of the Nisto Enterprise Web Application will be tested using the restored data.

4. Documentation: The data recovery process will be documented to ensure that it can be repeated in the future if necessary.

5. RISK MANAGEMENT POLICY

Introduction

This Risk Management Policy outlines the procedures and policies that will be used to manage risks associated with the Nisto Enterprise Web Application. The goal of the policy is to minimize the impact

of risks on the application and to ensure that the application continues to function effectively and efficiently.

Scope

This policy applies to all aspects of the Nisto Enterprise Web Application, including user data, system data, and configuration data. The policy covers the identification, assessment, and management of risks associated with the application.

Risk Assessment

The following steps will be taken to assess risks associated with the Nisto Enterprise Web Application:

1. Identification: Risks will be identified by conducting a thorough review of the application and its associated data, processes, and systems.

2. Assessment: Risks will be assessed in terms of their likelihood and impact, to determine the overall level of risk associated with each risk.

3. Prioritization: Risks will be prioritized based on their overall level of risk, to determine which risks require the most attention and resources.

Risk Management

The following steps will be taken to manage risks associated with the Nisto Enterprise Web Application:

1. Mitigation: Risks will be mitigated by implementing controls and procedures to minimize the likelihood and impact of risks.

2. Monitoring: Risks will be monitored to ensure that they are effectively managed and to detect any changes in the risk environment.

3. Review: The risk management process will be reviewed regularly, to ensure that it is effective and efficient, and to identify any changes that need to be made.

6. THIRD-PARTY SECURITY ASSESSMENT POLICY

Introduction

This Third-Party Security Assessment Policy outlines the procedures and policies that will be used to assess the security of third-party components and services used by the Nisto Enterprise Web

Application. The goal of the policy is to ensure that third-party components and services used by the application are secure and meet the security requirements of the enterprise.

Scope

This policy applies to all third-party components and services used by the Nisto Enterprise Web Application, including software libraries, cloud services, and other external services. The policy covers the assessment of third-party components and services to ensure that they meet the security requirements of the enterprise.

Assessment Criteria

The following criteria will be used to assess the security of third-party components and services used by the Nisto Enterprise Web Application:

1. Confidentiality: The confidentiality of data processed by the third-party component or service must be maintained.

2. Integrity: The integrity of data processed by the third-party component or service must be maintained.

3. Availability: The availability of the third-party component or service must be maintained.

4. Compliance: The third-party component or service must comply with applicable security standards and regulations.

5. Vulnerability Management: The third-party component or service must have a process in place for managing vulnerabilities.

Assessment Process

The following steps will be taken to assess the security of third-party components and services used by the Nisto Enterprise Web Application:

1. Identification: Third-party components and services will be identified by conducting a thorough review of the application and its associated data, processes, and systems.

2. Assessment: Third-party components and services will be assessed using the criteria outlined in this policy, to determine if they meet the security requirements of the enterprise.

3. Remediation: If necessary, third-party components and services will be remediated to ensure that they meet the security requirements of the enterprise.

4. Monitoring: Third-party components and services will be monitored to ensure that they continue to meet the security requirements of the enterprise.

7. BUSINESS CONTINUITY PLAN

Introduction

This Business Continuity Plan outlines the procedures and policies that will be used to ensure the continuity of the Nisto Enterprise Web Application in the event of a disaster or other disruptive event. The goal of the plan is to minimize the impact of disruptions on the application and to ensure that the application continues to function effectively and efficiently.

Scope

This plan applies to all aspects of the Nisto Enterprise Web Application, including user data, system data, and configuration data. The plan covers the steps that will be taken to ensure the continuity of the application in the event of a disaster or other disruptive event.

Disaster Recovery

The following steps will be taken to ensure the continuity of the Nisto Enterprise Web Application in the event of a disaster or other disruptive event:

1. Data Backup: Regular backups of all critical data will be made to ensure that data can be recovered in the event of a disaster.

2. Disaster Recovery Site: A disaster recovery site will be established to provide a backup location for the Nisto Enterprise Web Application in the event of a disaster.

3. Testing: The disaster recovery procedures and processes will be tested regularly to ensure that they are effective and efficient.

4. Communication: Communication procedures will be established to ensure that all stakeholders are informed of the status of the Nisto Enterprise Web Application in the event of a disaster.

5. Documentation: Detailed documentation of the disaster recovery procedures and processes will be maintained to ensure that they can be easily followed in the event of a disaster.

Business Continuity

The following steps will be taken to ensure the continuity of the Nisto Enterprise Web Application in the event of a disruptive event:

1. Business Impact Analysis: A business impact analysis will be conducted to determine the impact of a disruptive event on the Nisto Enterprise Web Application.

2. Continuity Strategies: Continuity strategies will be developed to ensure that the Nisto Enterprise Web Application can continue to function effectively and efficiently in the event of a disruptive event.

3. Emergency Response Plan: An emergency response plan will be established to ensure that the appropriate steps are taken in the event of a disruptive event.

4. Communication: Communication procedures will be established to ensure that all stakeholders are informed of the status of the Nisto Enterprise Web Application in the event of a disruptive event.

8. CHANGE MANAGEMENT POLICY

Introduction

The Nisto Enterprise Web Application is a critical component of the enterprise, and it is essential that changes to the application are managed effectively to ensure the stability and reliability of the application. This Change Management Policy outlines the procedures and policies that will be used to manage changes to the Nisto Enterprise Web Application.

Scope

This policy applies to all changes to the Nisto Enterprise Web Application, including changes to the code, configuration, and data. The policy covers the steps that will be taken to ensure that changes to the application are managed effectively and that the stability and reliability of the application are not impacted.

Change Management Process

The following steps will be taken to manage changes to the Nisto Enterprise Web Application:

1. Change Request: Changes to the Nisto Enterprise Web Application will be initiated by the submission of a change request. The change request should describe the change that is being proposed, the reason for the change, and the impact of the change on the application.

2. Approval: The change request will be reviewed and approved by the appropriate stakeholders, including the IT department, business users, and management.

3. Implementation: Once the change request has been approved, the change will be implemented. The implementation of the change should be carefully planned and monitored

to ensure that the impact of the change on the application is minimized.

4. Testing: The change will be tested to ensure that it is functioning as expected and that the stability and reliability of the application are not impacted.

5. Deployment: The change will be deployed to the production environment once it has been tested and approved.

6. Documentation: Detailed documentation of the change will be maintained, including a description of the change, the reason for the change, and the impact of the change on the application.

Reverting Changes

In the event that a change to the Nisto Enterprise Web Application is not functioning as expected, or is causing issues with the stability and reliability of the application, the change will be reverted. The following steps will be taken to revert the change:

1. Identification: The issue with the change will be identified and documented.

2. Analysis: The impact of the change on the application will be analyzed to determine the cause of the issue.

3. Reversion: The change will be reverted to the previous version of the application.

4. Testing: The application will be tested to ensure that the issue has been resolved and that the stability and reliability of the application are not impacted.

5. Deployment: The reverted version of the application will be deployed to the production environment once it has been tested and approved.

9. MONITORING AND LOGGING POLICY

Introduction

The Nisto Enterprise Web Application is a critical component of the enterprise, and it is essential that the application is monitored and logged effectively to ensure its stability and reliability of the application. This Monitoring and Logging Policy outlines the procedures and policies that will be used to monitor and log the Nisto Enterprise Web Application.

Scope

This policy applies to all monitoring and logging activities for the Nisto Enterprise Web Application, including the monitoring of the application's performance, availability, and security. The policy

covers the steps that will be taken to ensure that the application is monitored and logged effectively and that any issues with the application are detected and resolved in a timely manner.

Monitoring and Logging Process

The following steps will be taken to monitor and log the Nisto Enterprise Web Application:

1. Performance Monitoring: The performance of the Nisto Enterprise Web Application will be monitored to ensure that the application is functioning as expected and that the response time and availability of the application are within acceptable limits.

2. Availability Monitoring: The availability of the Nisto Enterprise Web Application will be monitored to ensure that the application is accessible to users and that any issues with the application are detected and resolved in a timely manner.

3. Security Monitoring: The security of the Nisto Enterprise Web Application will be monitored to ensure that the application is protected from unauthorized access, and that any security incidents are detected and resolved in a timely manner.

4. Logging: Detailed logs of all activity on the Nisto Enterprise Web Application will be maintained, including information on performance, availability, and security.

5. Alerts: Alerts will be generated when specific events occur on the Nisto Enterprise Web Application, such as performance degradation, availability issues, or security incidents. The alerts will be reviewed and acted upon in a timely manner.

6. Reporting: Regular reports on the performance, availability, and security of the Nisto Enterprise Web Application will be generated and reviewed by the appropriate stakeholders.

10. EMPLOYEE TRAINING POLICY

Introduction

The Nisto Enterprise Web Application is a critical component of the enterprise, and it is essential that all employees who use the application are trained on its features, functionality, and security measures. This Employee Training Policy outlines the procedures and policies that will be used to train employees on the Nisto Enterprise Web Application.

Scope

This policy applies to all employees who use the Nisto Enterprise Web Application, including full-time employees, contractors, and temporary workers. The policy covers the steps that will be taken to

ensure that employees are trained on the application effectively and that they have the necessary knowledge and skills to use the application in a secure and efficient manner.

Training Process

The following steps will be taken to train employees on the Nisto Enterprise Web Application:

1. New Employee Orientation: All new employees will receive training on the Nisto Enterprise Web Application as part of their new employee orientation. The training will cover the features and functionality of the application, as well as its security measures.

2. On-going Training: Regular training sessions will be conducted for all employees who use the Nisto Enterprise Web Application. The training sessions will cover new features and functionality of the application, as well as any updates to its security measures.

3. Online Training: Online training resources will be made available to all employees who use the Nisto Enterprise Web Application. The online training resources will include tutorials, videos, and interactive modules that will help employees to understand the features and functionality of the application, as well as its security measures.

4. Refresher Training: Refresher training sessions will be conducted on a regular basis to ensure that employees are up-to-date with the latest features and functionality of the Nisto Enterprise Web Application, as well as any updates to its security measures.

11. CONTINUOUS MONITORING PLAN

Introduction

The Nisto Enterprise Web Application is a critical component of the enterprise, and it is essential that the application is continuously monitored to ensure its security and availability. This Continuous Monitoring Plan outlines the procedures and policies that will be used to monitor the Nisto Enterprise Web Application, and to detect and respond to any security incidents.

Scope

This plan applies to the Nisto Enterprise Web Application, and it covers all aspects of the application, including its infrastructure, data, and software components. The plan will be reviewed and updated regularly to ensure that it remains relevant and effective in addressing the evolving security threats facing the enterprise.

Monitoring Process

The following steps will be taken to continuously monitor the Nisto Enterprise Web Application:

1. Event Log Monitoring: Event logs will be monitored in real-time to detect any unusual activity or security incidents. The event logs will be analyzed using automated tools and techniques to identify potential security threats and incidents.

2. Network Monitoring: The network infrastructure that supports the Nisto Enterprise Web Application will be continuously monitored to ensure its availability and to detect any potential security incidents.

3. Application Monitoring: The Nisto Enterprise Web Application will be monitored to detect any performance issues or potential security incidents. Automated tools and techniques will be used to identify any potential security threats and to trigger an incident response if necessary.

4. Data Monitoring: The data stored in the Nisto Enterprise Web Application will be monitored to ensure its integrity and to detect any potential security incidents. Automated tools and techniques will be used to identify any potential data breaches or unauthorized access to sensitive information.

Incident Response

In the event of a security incident, the following steps will be taken to respond to the incident and to minimize its impact:

1. Incident Triage: The incident will be triaged to determine its severity and to assign a priority for response.

2. Incident Containment: The incident will be contained to minimize its impact and to prevent it from spreading to other parts of the enterprise.

3. Incident Investigation: An investigation will be conducted to determine the cause of the incident and to identify any potential indicators of compromise.

4. Incident Resolution: The incident will be resolved, and any necessary remediation steps will be taken to restore the security and availability of the Nisto Enterprise Web Application.

5. Post-Incident Review: A post-incident review will be conducted to assess the effectiveness of the incident response process and to identify any areas for improvement.

12. DISASTER RECOVERY PLAN

Introduction

The Nisto Enterprise Web Application is a critical component of the enterprise, and it is essential that the application is protected against disasters that could cause significant downtime or data loss. This Disaster Recovery Plan outlines the procedures and policies that will be used to recover the Nisto Enterprise Web Application in the event of a disaster.

Scope

This plan applies to the Nisto Enterprise Web Application, and it covers all aspects of the application, including its infrastructure, data, and software components. The plan will be reviewed and updated regularly to ensure that it remains relevant and effective in addressing the evolving disaster scenarios facing the enterprise.

Disaster Recovery Process

The following steps will be taken to recover the Nisto Enterprise Web Application in the event of a disaster:

1. Disaster Declaration: The disaster will be declared, and the Disaster Recovery Team will be activated to respond to the disaster.

2. Disaster Assessment: The Disaster Recovery Team will assess the extent of the disaster and its impact on the Nisto Enterprise Web Application.

3. Disaster Mitigation: The Disaster Recovery Team will take any necessary steps to mitigate the impact of the disaster on the Nisto Enterprise Web Application.

4. Disaster Recovery: The Nisto Enterprise Web Application will be recovered, and any necessary data will be restored. The Disaster Recovery Team will ensure that the application is returned to its normal operating state as quickly as possible.

5. Disaster Verification: The Disaster Recovery Team will verify that the Nisto Enterprise Web Application is operating correctly, and that all data and critical services have been restored.

6. Disaster Review: A disaster review will be conducted to assess the effectiveness of the disaster recovery process and to identify any areas for improvement.

Disaster Recovery Teams

The following teams will be responsible for responding to disasters and recovering the Nisto Enterprise Web Application:

1. Disaster Recovery Team: The Disaster Recovery Team will be responsible for responding to disasters and recovering the Nisto Enterprise Web Application. The team will be composed of technical experts and key personnel from across the enterprise.

2. Data Recovery Team: The Data Recovery Team will be responsible for recovering any lost data and restoring the integrity of the data stored in the Nisto Enterprise Web Application.

3. Infrastructure Recovery Team: The Infrastructure Recovery Team will be responsible for recovering the infrastructure components that support the Nisto Enterprise Web Application.

Disaster Recovery Site

The Nisto Enterprise Web Application will be protected by a disaster recovery site, which will be used to recover the application in the event of a disaster. The disaster recovery site will be designed to provide a high level of availability and to ensure that the Nisto Enterprise Web Application can be recovered quickly in the event of a disaster.

13. Technology, Infrastructure, Privacy, and Terms of Use Policies

Introduction

The Nisto Enterprise Web Application and related applications are supported by best-in-class technologies and tools that provide the most secure, scalable solutions to your organization, wherever you exist.

Infrastructure

1. Nisto Enterprise - All first-party compute and storage resources are provided by Microsoft Azure and placed in the country of origin

2. All wireline communications between components use 128-bit encrypted SSL/TLS

3. Data is replicated across data centers by default for high availability

4. Data is encrypted at rest with AES-256 encryption, with security practices adhering to Microsoft's SDL

5. Tenant data is logically separated from each other using standard network traffic and application restrictions

6. System Uptime and Reliability can be viewed here.

7. Privacy Policy can be found here.
8. Terms of Use can be found here.