Approver: Todd Saunders, VP of Information Technology	**Policy Name:** Information Security Policy
	Version: 7.0
Effective Date: **April 24, 2018**	**Next Review Date:** **April 24, 2019**
Approver	**Date**

Oneida Nation Enterprises, LLC
Information Technology

Information Security Policy

The objective of the *Information Security Policy* is to ensure business continuity of Oneida Nation Enterprises, LLC and minimize risk of damage by preventing security incidents and reducing their potential impact.

Oneida Nation Enterprises expects all information users who have access to and responsibilities for information to manage it according to the procedures and security standards as set forth in this and other Policies.

DOCUMENT CHANGE CONTROL				
Ver. #	**Date**	**Policy Owner**	**Policy Contact**	**Change Description**
1.0	12/11/2014	VP of Technology and Supply Chain	IT Security Manager	
2.0	10/2015	VP of Technology and Supply Chain	IT Security Manager	Rev. for compliance to ISO27002 & PCI v3.1
3.0	5/2016	VP of Information Technology	IT Security Manager	Rev. for PCI v3.2 & NIST 800-53 rev4
4.0	5/3/2017	VP of Information Technology	IT Security Manager	Revised sections 9.2, 9.3& References for PCI v 3.2
5.0	12/13/17	VP of Information Technology	IT Security Manager	Revised Section 9 Introduction for NIST 800-171
6.0	3/28/2018	VP of Innovation	IT Security Manager	Revised Section 7
7.0	4/24/2018	VP of Innovation	IT Security Manager	Added PCI DSS responsibilities in section 5.
7.1	1/28/2019	VP of Innovation	Director for Information Security	Wording to align with compliance

Table of Contents

1. Introduction

Information security practices and standards serve to preserve and protect Oneida Nation Enterprises, LLC information assets. This policy documents and enumerates a set of requirements for protecting computers, systems and networks along with safeguarding information.

The integration of information technologies in every aspect of transmission and storage of ONE information requires responsible administrative, technical and physical security practices, standards and controls.

2. Scope

Information security applies to all areas for which ONE IT is responsible. It does not supersede any other policies published by areas of Oneida Indian Nation outside of Information Technology. All employees of Oneida Nation Enterprises, LLC are responsible for adhering to this Policy.

3. Objective

Information Security is defined as the preservation/protection of information assets to ensure:

- Confidentiality – Information is accessible only to those with authorization for access.
- Integrity – Ensuring accuracy and completeness of information and information processing methods.
- Availability – Authorized users have access to information and information systems in a timely manner.

Information exists in many forms; paper (hardcopy), digital, electronic, etc. Whatever form information takes, the objective of this Policy is to ensure that it is always safeguarded.

4. Principles of Information Security

Oneida Nation Enterprises, LLC Information Security program is built upon a set of principles that provide a basis for:

- Safeguarding confidential information in all formats, such as databases, email, paper documents;
- Protecting business applications;
- Securing all types of computing devices, ranging from networking systems, computers, and hand-held devices;
- Ensuring business communications remain on Oneida Nation Enterprises, LLC equipment;
- Protecting business communications networks, including wired & wireless, Voice over IP (VoIP), and Internet connectivity;
- Facilitating discussions with 3rd parties when establishing contracts or service level agreements governing information security arrangements.

These principles also map to security-related standards and best practices.

Security requirements for information resources are determined by an assessment of risk. Not all information resources require the same level of security or protection. Controls specified by policies, standards, and procedures assume that application of security measures are commensurate with the confidentiality of the information resource being protected.

5. Roles and Responsibilities

Information (Data) Stewards
(e.g., HR is an information steward of Kronos, Bingo is an information steward of Video King)

Oneida Nation Enterprises, LLC Information Stewards assume responsibility for the management practices of information they control and manage. This includes, but is not limited to, inventory of the information for which responsible, classification of information, and authorization for access to the information. Department Directors have the responsibility to implement this policy within their units. Information Stewards must comply with this policy and the baseline standards for computer security and the technical requirements for the protection of confidential and restricted information.

Information Users

Information Users are individuals who have been granted access to specific information resources to successfully complete their assigned duties. Information Users can include, employees, staff, contractors, consultants, etc.

Information Users must:

- Review, understand and comply with the policies, standards, and procedures that comprise this Policy;
- Agree in writing to this Policy;
- Participate in security awareness training annually;
- Immediately notify the Help Desk or the Information Security Office of any known or suspected information security incident or issue.

Office of Information Technology

Office of Information Technology is responsible for:

- Ensuring that information technology architecture components are designed and implemented to protect the information they process in accordance with the policies, standards, and procedures that constitute this Policy;
- Define, implement, and test disaster recovery plans and make contingency arrangements to manage the prolonged unavailability of critical computer facilities, equipment, or communications services;
- Maintain an accurate and up-to-date inventory of information system hardware and software;
- Ensure that all implementations, maintenance, enhancements, and other activities are conducted in accordance with the policies, standards, and procedures that constitute this Policy;
- Create, maintain and publish an *Information Security Policy*, supported by documented standards and procedures as appropriate based upon industry best practices and reviewed annually.

Vice President of Innovation

- Develops, documents, implements and maintains an Oneida Nation Enterprises, LLC Information Security Program to ensure that ONE meets information security requirements and regulations;

- Develops, documents, implements and maintains Oneida Nation Enterprises, LLC information security policies, procedures, and control techniques to provide direction for implementing the requirements of the Information Security Program;
- Provides training and oversight to personnel with significant information security responsibilities and with respect to such responsibilities;
- Assists senior executives and other key official with understanding and implementing their information security responsibilities;
- Establishes minimum mandatory risk based technical, operational, and management information security control requirements for Oneida Nation Enterprises, LLC information and information systems;
- Reports compliance failure or policy violations directly to appropriate officials for appropriate disciplinary and corrective actions;
- Ensures senior information officials comply with all Oneida Nation Enterprises, LLC Information Security Program requirements and ensures they have all necessary authority and means to direct full compliance with such requirements;
- Develops, implements and maintains capabilities for detecting, reporting and responding to information security incidents;
- Designates a Senior Information Security Officer to carry out responsibilities relevant to information security.

Information Technology Security Officer

- Provides recommendations to VP of Innovation referencing information security;
- Maintains professional qualifications required to administer the functions of the Information Security Program;
- Develops, documents, implements and maintains Information Security Program to protect Oneida Nation Enterprises, LLC information assets and information systems;
- Develops, documents, implements and maintains well-designed, well-managed continuous monitoring and standardized risk assessment processes;
- Performs independent oversight and governance functions for information assurance and protection, information risk management, security incident response investigations, business continuity, and disaster recovery;
- Seeks guidance from General Counsel to interpret regulations involving information security and privacy;
- Produces and maintains information security policies and standards that recommend information security measures and controls;
- Develops methodologies and processes for compliance to information security policies and standards that are effective and consistent;
- Reviews and validates compliance reports from external vendors;
- Provides expertise and knowledge of trends in information security and business continuity to improve control processes across Oneida Nation Enterprises, LLC;
- Responds, investigates, and reports on information security incidents.

Information Technology Directors and Managers

- Ensure effective processes and procedures are established to implement the policies, procedures, control techniques, and other countermeasures identified in the Information Security Program;

- Coordinate with VP of Innovation and Information Security Officer and others involved with securing Oneida Nation Enterprises, LLC information assets and systems to ensure they are adequately secure and risks are managed to an acceptable level;
- Ensure system controls are continuously monitored, operating as expected and adequately protecting information assets;
- Coordinate with the Information Security Officer in responding to information security data calls, audit requests, and reporting;
- Ensure continuous compliance with all requirements to which ONE must adhere, i.e. PCI DSS, PII, GDPR, NIST, CALEA, HIPAA, etc.

6. Information (Data) Classification

The information (data) classification level determines the security controls that must be applied to protect an information asset, and the procedures that must be followed when acquiring, storing, using, transmitting, archiving, and destroying the information asset.

This policy establishes three levels of information security classifications:

1. Confidential
2. Restricted
3. Public

Confidential Information

Information classified as confidential information may be subject to legal or regulatory requirements that go beyond those given here. For example, credit card transactions are subject to the Payment Card Industry Data Security Standard (PCI DSS) and personal medical information is subject to HIPAA.

Information that has been determined by Oneida Nation Enterprises, LLC information stewards to require the highest level of privacy and security controls is considered confidential information. Any information containing any of the following data elements, when appearing in conjunction with an individual's name or other identifier, is considered to be confidential information:

- Social Security number
- Credit Card number
- Driver's license number
- Passport
- Bank account number
- Protected health information (as defined in the Health Insurance Portability and Accountability Act HIPAA)
- Guest Information – Identification of guests and private information
- Intellectual Property
- Nation Data – membership roles, etc.
- HR Data – Private information about employees
- Legal Data – Litigation in progress or attorney-client communications
- passwords – as they allow access to systems that can contain confidential information

Technical safeguards around confidential information are required by this policy. Information stewards/custodians may require employees to apply these technical standards to other or additional types of information. This policy does not limit this practice.

* *Note: Individuals storing personal information on company assigned computers are not within the requirements for safeguarding confidential data.*

Restricted Information

Unless otherwise classified, all information used to conduct Oneida Nation Enterprises, LLC business is restricted.

Public Information

Oneida Nation Enterprises, LLC publically available or published information for the explicit use of the general public.

7. Information (Data) Handling Requirements

Confidential / Restricted:

For the purposes of this policy, a system is considered to be "holding" confidential information when such information is stored locally on the system, when the system accesses any storage volume containing such information, or when the system is used to process, analyze, or transmit such information.

The following requirements apply to any system that holds confidential or restricted information (as classified in this policy).

- information must only be provided on a need-to-know basis in accordance with data handling best practice – *"Least Privilege";*
- all media storing information must be classified as to type;
- all media backups containing confidential information must be stored in a secure location and the physical security of the location must be reviewed annually;
- media containing confidential information must be transported by a delivery method that can be accurately tracked;
- management must approve all media containing confidential information that is moved from a secured area;
- inventory logs must be kept of all media containing confidential information and reviewed annually;
- media storing confidential information that is no longer needed for business or legal requirements must be destroyed so that data cannot be reconstructed;
- hardcopy materials storing confidential data must be shredded, incinerated, or pulped so that data cannot be reconstructed;
- encryption may be required to protect information either at rest or in transit;
- Information Security Office will approve a given method of encryption for use with confidential data; it must employ an established contemporary algorithm (TLS 1.2 or stronger);
- any system containing confidential data that leaves Oneida Nation Enterprises, LLC. facilities must be encrypted;
- laptops and mobile devices must be encrypted;

- any system that is used in a facility that is not physically secured, that contains confidential data must be encrypted;
- systems containing confidential data must keep all software up-to-date;
- appropriate end-point protection must be installed, active, and current;
- systems must be secured according to established industry best practices;
- all network services not needed for the system to fulfill its functions must be disabled;
- password defaults must be changed;
- an open website must not be run on a system holding confidential information;
- logging must be activated and follow retention policy;
- file integrity software must be installed and activated;
- confidential information stored locally on a system must be removed when no longer needed for operational reasons;
- any confidential information on development and/or test systems must be masked or redacted;
- any system accessing confidential information via a wireless network or any remote, off-site access to a system containing such data must use an encrypted or secured communication method (TLS 1.2 or stronger);
- all business email communications must only be conducted using company provided email services;
- confidential information must be encrypted when it is transmitted via email;
- credit card data (including PANs) may never be transmitted via end-user messaging technologies;
- confidential information may not be transmitted via instant messaging or text messaging;
- confidential information must be encrypted when it is accessed via the Web; and
- passwords or encryption keys used to access confidential data must be protected in the same manner as confidential information and are subject to Data handling via this Policy.

Media Handling:

All records, regardless of storage location, will be retained only as long as required for legal, regulatory, and business requirements. The specific retention length will be established by General Counsel, appropriate business unit and the data owner or system administrator. When a complaint is received or when litigation is probable, General Counsel may suspend automated email programs or recycling of back-up media.
Upon verification that a business requirement for hardware that no longer holds confidential information, no longer exists or is being met through an effective and appropriate alternative, the electronic storage media must be degaussed and a certificate received verifying physical destruction of the drive.

Type of Record	Owner	Usage	Minimum	Requirements
Contracts	General Counsel	Service Provider Agreement	Duration of contract	
Credit Cardholder Information	VP of Finance	single or recurring transactions	7 years	1 yr. after fiscal yr.
IT Audit logs	VP of Innovation	Network and System audit logs	90 days online / 1 year offline	PCIDSS 3.2
Accounting Records	VP of Finance	gaming transactions	7 yr.	Nation-State Compact
Remote Access Logs	OINGC	Remote Access To Gaming network	5 yr.	OINGC MICS, Chapter 13
Security Logs	OINGC		5 yr.	OINGC MICS, Chapter 13

Restricted

- information must only be provided on a need-to-know basis in accordance with data handling best practice – *"Least Privilege";*
- information location (data at rest) must be sufficiently protected from any unauthorized access;
- non-disclosure agreements must be signed prior to making information available to 3rd parties;

Media handling:

- information on computer systems must be protected by access controls and meet minimum policy standards;

Public

- Public information must be approved for release by the appropriate manager.

Media handling:

- none

Paper Document Security

Anyone handling confidential information in hard copy should take all appropriate measures to secure it physically. It should be stored in a locked office or cabinet and when in use, closely supervised. The following measures are mandatory for paper documents containing confidential information.

1. Locked in drawer, file cabinet, office.
2. Never leave confidential information unattended in a public area.
3. When no longer needed must be destroyed or moved to secure archive facility.
4. When transmitted a receipt of delivery is required.
5. When transmitted by inter-office mail, envelope must be sealed and stamped "confidential".
6. Destroying confidential documents requires secure disposal service or cross-cut shredder.

Printer Security

1. Personal code is recommended to print documents.
2. Code must not be shared with other users.
3. Printer should be in a location where it is accessible only to authorized personnel.
4. Off-hours the printer has to be in a physically locked environment.
5. Periodically the printer queue should be audited to ensure only authorized users have accessed the device and all documents are accounted for.
6. Confidential printed documents should not be left on the printer after printing.

8. Improper Custodianship

You must not access, manipulate, or change data without prior authorization from your supervisor. In addition, you may only access, manipulate, or change data as required to fulfill your assigned duties. Suspected violations will be investigated by the appropriate office, and disciplinary measures may be taken in accordance with applicable regulations or policy.

These examples are illustrative, not exhaustive of inappropriate data access:

- Do not change data about yourself or others for other than usual business purposes.
- Do not use information (even if authorized to access it) to support actions by which individuals might profit (e.g., a change in salary, title, etc.).
- Do not disclose information about individuals without prior supervisor authorization.
- Do not engage in what might be termed “administrative voyeurism” (e.g., tracking the pattern of salary raises; determining the source and/or destination of telephone calls or Internet protocol addresses;), unless authorized to conduct such analyses.
- Do not circumvent the nature or level of data access given to others by providing access or data sets that are broader than those available to them via their own approved levels of access, unless authorized.
- Do not facilitate another's illegal access to Oneida Nation Enterprises, LLC administrative systems or compromise the integrity of the system data by sharing your passwords or other information.
- Do not violate Oneida Nation Enterprises, LLC policies in accessing, manipulating, or disclosing administrative data.

9. Baseline IT Security Requirements

Introduction

To safeguard Oneida Nation Enterprises, LLC information assets and information technology (IT) resources, ONE Information Security Office requires the following practices. These requirements apply to any system that is used to conduct Oneida Nation Enterprises, LLC business or is connected to the business network.

Only authorized devices will be permitted on the network.

Any system that poses an unacceptable risk to the stability, performance, and security of the network will be declared unauthorized and removed.

Requirements for securing confidential information reflects an approach referred to as “defense-in-depth”. Defense-in-depth is a “best practice” strategy for protecting information and relies on techniques and technologies that currently exist. It requires a balanced focus on participation from users, configuration of appropriate technology, and actively monitoring activity for ‘abnormal’ behavior.

9.1 Baseline Requirements for all systems:

- Computers must have screen lock-out enabled;
- All relevant operating system, server, and application software must be patched and up-to-date;
- All critical and security software patches must be installed no later than 1 month from release;
- User privilege will be configured as low as possible while still meeting operational needs *“Least Privilege”*;
- All accounts must have strong passwords;
- Electronic distribution of passwords must be sent encrypted;

- Local operating system firewalls must be enabled and running, and users must not be able to alter settings;
- End-point protection must be installed with updates and active protection enabled;

9.2 Baseline Requirements specific to Application and File Servers

- Operating system and all software applications must be secured according to industry best practices;
- Servers must operate with only the minimum software and application specific features that are necessary for the system to perform its function;
- Default passwords set by the vendor must be changed;
- Shared accounts are prohibited, except where it is not technically possible to provision individual accounts;
    - where a share account is necessary a local inventory of who has access must be maintained;
    - password for shared account must be changed whenever there is a change in personnel or access requirements;
- Servers must be on a segregated network from users;
- All critical and security software patches must be installed no later than 1 month from release;
- End-point protection must be installed with updates and active protection enabled;
- File Integrity software must be installed on servers with compliance requirements;
- Logging must be enabled and being sent to SIEM;
- All servers must be scanned quarterly to assess susceptibility to vulnerabilities;
- All configuration changes must follow *Change Control Policy*.

9.3 Baseline Requirements for Web Servers

Web server applications must adhere to the baseline Requirements specific to Application and File Servers. In addition they must also adhere to the following:

- Must not store any confidential data that is not protected;
- Must not store any cardholder data;
- All development, test and/or custom application accounts must be removed prior to production release;
- File Integrity software must be installed on servers with compliance requirements;
- Must not store any confidential data that is not protected;
- All development, test and/or custom application accounts must be removed prior to production release;
- Web servers must be scanned quarterly to assess susceptibility to vulnerabilities;
- All configuration changes must follow *Change Control Policy*.

9.4 Baseline Requirements for Database Servers

Databases containing cardholder data must have access restricted to the following:

- All user access, user queries, and user actions on databases are through programmatic methods;
- Direct access or query of databases is restricted to database administrators;
- Application IDs for database applications can only be used by the application (not individual users or other non-application processes;

9.5 Baseline Requirements for Handheld Devices

Handheld devices include smartphones, tablets, or other mobile devices used to conduct business which pose an acceptable risk to the stability, performance, and security of the network**.** In addition to baseline requirements for all systems, handheld devices must adhere to the following:

- Any handheld device that is configured to be used for business, including retrieval of email or calendaring information must be configured so that it can be locked or erased if it is lost or stolen;
- Configure device to lock the console after a period of inactivity no greater than 15 minutes;
- Password is required to unlock the device.

9.6 Baseline Requirements for Specialized Devices

A specialized device is electronic equipment that is used on a network, such as printers, copiers, facsimile machines, network systems, or other control systems.

- Vendor-defined security or critical software or firmware updates must be applied within 30 days of their release;
- Passwords must be changed from vendor-supplied;
- Where technically feasible, passwords must meet complexity requirements;
- Vendor-supplied accounts not necessary for maintenance support, or device functionality must be locked or disabled;
- Remote use or administration must be performed via secure remote access mechanisms;
- When devices are removed from service, any persistent storage must be erased or destroyed;
- Network segregation is required to separate these devices from systems containing confidential information (data).

9.7 Baseline Requirements for Network Security

- Implement network access controls and a firewall for the Oneida Nation Enterprises, LLC. network;
- Logging must be enabled that adheres to best practices;
- A vulnerability scanning tool should be run every six months on all networking segments to assess and remediate high-risk vulnerabilities;
- Network must be segmented to isolate workstations, servers, and control appliances;
- Unused network jacks/ports must be disabled;

9.8 Baseline Security for payment card data devices

- Inventory must be maintained of all devices including the following:
  - make and model;
  - physical location of device;
  - device serial number or other unique identifier.
- Devices must be periodically inspected to detect for tampering or substitution;
- Personnel must be trained for tampering awareness:
  - verify identity of 3rd party maintenance personnel prior to granting access;
  - installation, replacement or returns must have device verified;
  - be aware of suspicious behavior around devices;
  - report suspicious behavior and indications of device tampering or substitution to appropriate personnel.

9.9 Baseline Security for Hosted applications (SaaS)

- Must not store any confidential data that is not protected;
- Must not store any PCI cardholder data;
- All development, test and/or custom application accounts must be removed prior to production release;
- SaaS must provide SSAE 16 / SOC reports and other compliance reports annually;
- Compliance reports must be reviewed annually by ONE Information Security office.

10. Physical Security

Oneida Nation Enterprises, LLC Information Technology assets must be protected from physical tampering, misuse, damage or loss. Premises where IT equipment and assets are located will be protected from unauthorized physical access. Such protections will be consistent with the degree of risk and the need for compliance with applicable regulations or contractual obligations.

Proof of authorization to be present in areas where IT assets are located must be available at all times.

Where physical access is strongly constrained (data centers, server rooms, wiring closets, etc.) additional measures will be in place to enforce limits to entry, and to record entrance and purpose.

Persons requiring access will carry company-issued identification which will be clearly visible. Those individuals not authorized (vendors, facilities/maintenance, security, 3rd party, etc.) must be escorted at all times and sign in and out of the facility. In an emergency, refer to the Disaster Recovery Plan.

Unauthorized entry to any location will be recorded, investigated and reported to ONE IT senior management.

11. Monitoring & Auditing Information (Data)

Oneida Nation Enterprises, LLC information technology infrastructure, environments, systems, applications and data will be monitored to identify attempts to tamper with, damage, destroy, obtain without authorization, or steal any company information asset, whether physical or electronic in nature. ONE information technology department will maintain procedures and technologies for identifying such attempts. Procedures for responding to information breaches will be documented in the *Incident Response Policy*.

Records and evidence of information security events and alerting will be maintained in a manner that allows for their use in forensics investigations or referral to external parties for further action. Information security events will be reported to Oneida Nation Enterprises, LLC Information Security office for review.

The following information is required to be maintained:

- audit logs linking all user access to system components;
- automated audit trails for all system components to reconstruct the following events:
    - individual user access to cardholder data, confidential data;
    - all actions taken by any individual with root or administrative privileges;
    - access to all audit trails;

  - invalid logical access attempts;
  - changes to identification and authentication mechanisms (new accounts & elevation of privileges); and
  - all changes, additions or deletions to accounts with root or administrative privileges;
- any initialization, stopping or pausing audit logs;
- creation and deletion of system level objects;
- audit trail entries for all system components for the following:
  - user identification;
  - type of event;
  - date and time;
  - success or failure indication;
  - origination of event;
  - identity or name of affected data, system component, or resource;
- time synchronization for all critical system clocks and times and ensure the following:
  - critical systems have correct and consistent time;
  - time data is protected;
  - time settings are received from industry-accepted time sources;
- secure audit trails so they cannot be altered;
  - limit viewing of audit trails to those with job-related need;
  - protect audit trail files from unauthorized modification;
  - promptly back up audit trail files to centralized log server or media that is difficult to alter;
  - write logs for external-facing technologies into a log server;
  - use file integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts;

Daily reviews:

- all security events;
- logs of all system components that store, process or transmit cardholder data;
- logs of all critical system components;
- logs of all servers and system components that perform security functions;
- logs of all other system components based on policies and risk management strategy.

Log Retention:

- audit trail history must be maintained at least one year; and
- 90 days must be immediately available for analysis.

Exception Procedures

Computers or other IT resources that are not able to meet baseline security requirements must be reviewed and an exception obtained and documented containing the following information:

- Resource must be identified – hardware, operating system, application, purpose;
- Reason as to why the system is not able to meet baseline;
- Mitigation must be identified;
- Time Period assigned for the exception;
- Signature of the VP of Innovation and Information Security Officer;

A list of all exception systems will be kept with the above information and will be reviewed in accordance with the *Exception Policy*.

References

- *Exception Policy*
- *Change Control Policy*
- *Incident Response Policy*