# Revision History

<table>
<thead>
<tr>
<th>Changes</th>
<th>Approving Manager</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Publication</td>
<td></td>
<td>9/1/2009</td>
</tr>
<tr>
<td>Updates to more accurately reflect the UNR environment</td>
<td></td>
<td>9/30/2009</td>
</tr>
<tr>
<td>Update to match policy to agree with training</td>
<td></td>
<td>1/20/10</td>
</tr>
<tr>
<td>Update to match policy to agree with new websites</td>
<td></td>
<td>3/12/10</td>
</tr>
<tr>
<td>Update and review to version 2.0</td>
<td></td>
<td>11/1/2016</td>
</tr>
<tr>
<td>Update and review to version 3.0</td>
<td></td>
<td>9/28/2018</td>
</tr>
</tbody>
</table>

---

Steve Smith, Vice Provost for Information Technology

Date: 10-1-2018
# TABLE OF CONTENTS

1 INTRODUCTION ................................................................................................................................. 6  
   1.1 INTRODUCTION ........................................................................................................................... 6  
   1.2 TERMS ........................................................................................................................................ 6  

2 POLICY APPLICABILITY, DISTRIBUTION, & UPDATES ................................................................. 7  
   2.1 POLICY APPLICABILITY & DISTRIBUTION .............................................................................. 7  
      2.1.1 Off Premise, Cloud or Hosted Services or Systems ........................................................... 7  
      2.1.2 Information Security Awareness Training ........................................................................ 7  
   2.2 POLICY & SUPPORTING DOCUMENTATION UPDATES .......................................................... 7  
      2.2.1 Business Associate Agreements ......................................................................................... 8  

3 DATA CLASSIFICATION AND CONTROL POLICY .......................................................................... 9  
   3.1 DATA CLASSIFICATION .............................................................................................................. 9  
      3.1.1 Unrestricted Data ................................................................................................................ 9  
      3.1.2 Sensitive Data ...................................................................................................................... 9  
      3.1.3 Confidential Data .................................................................................................................. 9  
      3.1.4 Regulated Data ..................................................................................................................... 9  
   3.2 DATA COLLECTION .................................................................................................................... 10  
   3.3 DATA ACCESS ............................................................................................................................. 10  
   3.4 PHYSICAL SECURITY .................................................................................................................. 10  
      3.4.1 Access to Sensitive Areas and Equipment ........................................................................... 11  
      3.4.2 Escorted Only Access ........................................................................................................... 11  
      3.4.3 Public Access Areas with Equipment Storing or Transmitting Confidential or Regulated Data ................................................................................................................................... 12  
   3.5 USER MANAGEMENT .................................................................................................................. 12  
      3.5.1 Users .................................................................................................................................... 12  
      3.5.2 Terms of User Banner .......................................................................................................... 12  
      3.5.3 Password Resets ................................................................................................................... 12  
      3.5.4 Contractor/Vendor Accounts ............................................................................................. 12  

4 IT CHANGE CONTROL POLICY ...................................................................................................... 13  
   4.1 CHANGE MANAGEMENT .......................................................................................................... 13  
   4.2 MINIMUM CHANGE PROCESS .............................................................................................. 13  
   4.3 CHANGE TESTING ..................................................................................................................... 13  
   4.4 CHANGE IMPLEMENTATION .................................................................................................... 14
4.5 EMERGENCY CHANGES

5 DATA RETENTION AND DISPOSAL POLICY

5.1 RETENTION REQUIREMENTS

5.2 DISPOSAL REQUIREMENTS

6 PAPER AND ELECTRONIC MEDIA POLICIES

6.1 STORAGE

6.1.1 Physical Security

6.1.2 Hardcopy Media

6.1.3 Electronic Media

6.2 INVENTORY

6.3 DESTRUCTION

7 SYSTEM CONFIGURATION, SECURITY AND ADMINISTRATION POLICY

7.1 DEVICE MANAGEMENT RESPONSIBILITIES

7.2 BASELINE CONFIGURATION

7.3 CONFIGURATION CHANGES, UPDATES AND PATCHES

7.4 SECURITY VULNERABILITY & NETWORK SCANNING

7.5 RISK ASSESSMENTS

7.6 SECURITY CONTROL ENFORCEMENT

7.7 LOGS

7.8 AUDIT & ACCOUNTABILITY

7.9 MAINTENANCE

8 ELECTRONIC MEDIA BACKUP POLICY

8.1 LOCATION

8.2 TRANSPORT

8.3 AUDIT

8.4 MEDIA DESTRUCTION

9 ENCRYPTION POLICY

9.1 GENERAL ENCRYPTION REQUIREMENTS

9.2 TRANSMISSION OVER UNTRUSTED NETWORKS

9.3 ENCRYPTION OF WIRELESS NETWORKS

9.4 EMAIL TRANSMISSION OF SENSITIVE, CONFIDENTIAL OR REGULATED DATA

10 SOFTWARE DEVELOPMENT POLICY

10.1 SOFTWARE DEVELOPMENT: GENERAL USE DATA
10.2 SOFTWARE DEVELOPMENT: SENSITIVE OR CONFIDENTIAL DATA ........................................ 26
  10.2.1 Development Life-Cycle ............................................................................................... 26
  10.2.2 Web-based Applications ............................................................................................... 27
10.3 SOFTWARE DEVELOPMENT: REGULATED DATA .......................................................... 27

11 INCIDENT RESPONSE PLAN AND PROCEDURES ............................................................ 28
  11.1 INCIDENT RESPONSE REQUIREMENTS AND INFORMATION ..................................... 28
  11.2 BUSINESS CONTINUITY PLANS ................................................................................... 28
  11.3 AUTOMATED SECURITY SYSTEM NOTIFICATIONS ...................................................... 28

12 THIRD PARTIES AND THIRD PARTY AGREEMENTS ......................................................... 29
  12.1 UNRESTRICTED DATA AGREEMENTS ............................................................................. 29
  12.2 SENSITIVE, CONFIDENTIAL OR REGULATED DATA AGREEMENTS ............................. 29
1 INTRODUCTION

1.1 INTRODUCTION
These Information Security Policies and Procedures (ISPP) explain information security requirements for all University of Nevada, Reno (UNR) employees, students, contractors, vendors, third parties, and guests.

The ISPP will take precedence whenever not in conflict with any local, state, or federal laws, and Nevada System of Higher Education (NSHE) or other UNR requirements, policies and guidelines.

Any request for exemption from the ISPP, or any portion thereof must be submitted in writing to the Chief Information Security Officer for approval.

Failure to follow the ISPP may result in removal from the UNR network and/or revocation of access to UNR data.

1.2 TERMS
The following terms are offered to provide clarification of references made throughout the ISPP.

High Security Area: An area where equipment handling Sensitive, Confidential or Regulated Data resides or an area requiring badge access for entry.

OIT Staff: Staff members that manage IT computing resources campus-wide, or for a specific department or unit. NSHE: The Nevada System of Higher Education

NSHE Records Retention and Disposition Schedule: Chapter 18 of NSHE’s Procedures and Guidelines Manual, which can be accessed here: http://system.nevada.edu/tasks/sites/Nshe/assets/File/BoardOfRegents/Procedures/PGMCH18RECORDSRETENTIONANDDISPOSITIONSCHEDULE.pdf

PCI: Payment Card Industry; PCI data includes cardholder data relating to credit card processing.

System Configuration Guides: Policies created to provide configuration requirements for baseline systems and for protected systems, which are reviewed on a regular basis and updated as needed.

UNR: The University of Nevada, Reno, and all of its subsidiary departments.

User: Any employee, student, contractor, vendor, third-party, or guest that uses, maintains, or handles any UNR information system or network.
2 POLICY APPLICABILITY, DISTRIBUTION, & UPDATES

2.1 POLICY APPLICABILITY & DISTRIBUTION
The ISPP applies to all UNR computing resources, including all University owned, licensed, or managed hardware or software, and use of the University network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

All Users must follow the ISPP.

The ISPP and the supporting documents shall be made available to all Users that must follow and have knowledge of the policy.

Departments or units outside of OIT that manage their own computing resources and wish to implement similar policies and procedures to manage internally, may do so through the policy exemption process. (See Introduction). When exemptions are approved, it is the responsibility of the requested department or unit to properly communicate the exemption to all affected Users.

2.1.1 Off Premise, Cloud or Hosted Services or Systems
For all Software as a Service (SAAS), Platform as a Service (PAAS), Infrastructure as a Service (IAAS), or other services where Sensitive, Confidential or Regulated Data (as defined in Section 4.1) is stored, the service provider must meet all regulatory and state requirements for hosting that type of data. In the absence of any regulatory requirements, ISO 27001 standards apply.

The contracting department or unit is responsible for verifying and maintaining records of the service provider’s Attestations of Compliance (AoC).

For hosted or off premise virtual infrastructure (servers, network devices, appliances, etc.) all relevant baseline security configuration standards must be applied for the type of data stored or processed by the system.

2.1.2 Information Security Awareness Training
Employees must be adequately trained to carry out their assigned information security-related duties and responsibilities. All employees within UNR who have access to Regulated Data shall undergo annual information security awareness training to ensure they are aware of significant security issues that pose a threat to the organization as a whole. The training will be provided by the Information Security Department.

2.2 POLICY & SUPPORTING DOCUMENTATION UPDATES
The ISPP and the supporting documentation including procedures and definition documents will be evaluated at least annually and updated as required for continued business continuity and regulatory compliance. Evaluations will be performed by qualified persons and revisions documented accordingly. Any time the ISPP or supporting documents are updated or modified relevant changes will be distributed, and relevant training material updated to reflect the changes.
2.2.1 Business Associate Agreements

Business Associate Agreements (BAA’s) are required to transfer Health Insurance Portability and Accountability Act (HIPAA) and other Sensitive Data between UNR and 3rd parties. BAA’s will be reviewed as part of the contracting process for relevance and compliance as applicable to HIPAA & other regulatory data standards. BAA’s may be excluded when the receiving party or the data being transferred is exempted as outlined by HIPAA law.
3 DATA CLASSIFICATION AND CONTROL POLICY

3.1 DATA CLASSIFICATION

All data stored, transmitted, or processed through UNR’s computer systems will fall under one of four data classifications. The data owner or creator is responsible for data classification. When the data owner is not defined, the Department Head or Vice President of the area responsible for the data defaults as the data owner.

The data classifications are Unrestricted, Sensitive, Confidential and Regulated. In the event data is eligible for classification in more than one data classification level, the highest of the eligible data classification levels should be used. Data within a particular classification may be held to a higher security standard as required by certain governance requirements. Research data as well as business data may fall into any of the specified categories. For more information on data classification, security controls implementation, and governance requirements, please see the Data Classification Policy Guidelines and Matrix (Appendix A.3).

3.1.1 Unrestricted Data

Unrestricted Data is data that is used in normal day-to-day operations and does not contain any Sensitive information. Examples of this data would be general emails and communications to the public at large and data that would not qualify as Confidential or governed by any regulatory and/or compliance standard. It is important to note that while some forms of Unrestricted Data may be made available to the public, it is not freely disseminated without appropriate authorization from the data owner.

3.1.2 Sensitive Data

Sensitive Data is data that is not for general use though it may be widely distributed as needed and should be protected but is not governed by statute or regulation. Examples of Sensitive Data would include data that would cause loss of reputation, confidence, and/or has financial impact to UNR and other information deemed not for general release and use (subject to UNR’s obligations under public records law).

3.1.3 Confidential Data

Confidential Data is data that is governed by statutory, regulatory or contractual requirements that require protection of the data. Examples of Confidential Data would include Family Educational Rights and Privacy Act (FERPA), Graham Leach Bliley Act (GLBA), Personally Identifiable Information (PII), proprietary information, and biometric data. Unauthorized disclosure of this type of data could have a serious adverse impact on the University, individuals or affiliates.

3.1.4 Regulated Data

Regulated Data is data that is required by various regulatory compliance standards and/or local, state, and federal laws to be strictly and specifically protected. Regulated Data must be protected to the highest standards as applicable to the data governance requirements and whenever possible must be stored and accessed separately from lower data classifications. Examples of Regulated Data are Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), and Department of University of Nevada, Reno Information Security Policies and Procedures

Version 3.0 - September 2018 Copyright © 2018 University of Nevada, Reno All Rights Reserved.
Defense (DOD) data.

Regulated Data may also be referenced as Controlled Unclassified Information (CUI).

3.2 DATA COLLECTION
UNR collects various types of data during normal business operations; while UNR rarely collects packet level content outside of troubleshooting, some or all content may be collected, stored, and viewed as required for business operations. All data collected, stored, and viewed is done so in support of business operations, network monitoring, and for performing required security analytics. UNR will comply with local, state, and federal e-discovery requests as required by law.

3.3 DATA ACCESS
All data that is classified as Sensitive, Confidential or Regulated must be protected via appropriate access controls to ensure that data is not improperly disclosed, modified, deleted or rendered unavailable. Logs must track all access to such data and identify by whom and when the data was accessed when required by the appropriate system configuration guide.

Employees who have been authorized to view information at a particular classification level will only be permitted to access information at that level or at a lower level on a need-to-know basis. All access to systems must be configured to deny all but what a particular user needs to access per their business role (least privilege access).

Access to systems or applications handling Confidential or Regulated information must follow the data access request process. All requests require approval by the data owner and Information Security and must have a valid Authorization Request Form (Appendix C.2) on file. Access to data exceeding the employee’s authorized role must also follow the data access request process and must include documented limits around such access (e.g. access source, access time limits, etc.).

Prior to accessing systems or applications containing Regulated Data, individuals must undergo a standard background check by the Human Resources Department or a criminal background check by University Police Services, as applicable. When an employee who has access to Regulated Data is either terminated or transferred to another department, UNR OIT must be immediately notified and will suspend all access to such data.

In cases where access to an employee’s data files is necessary, including where the employee has separated from employment or is deceased, refer to the procedure for Granting Access to Employees Data Files (Appendix B.5).

3.4 PHYSICAL SECURITY
Hard copy materials and electronic media considered Sensitive, Confidential or Regulated (proprietary, PII, PCI, HIPAA, etc.) must be protected by appropriate physical access controls.

Cameras or other logged access control mechanisms must be used to monitor the entry and exit points of places when required for regulatory compliance (see System Configuration Guides). Video cameras or other mechanisms should be protected from tampering or disabling. The data collected must be
monitored and stored in accordance with the *Log Retention Policy* (Appendix A.2) and the NSHE Records Retention and Disposition Schedule unless otherwise restricted by a regulatory compliance standard or law.

Appropriate facility controls must be used to limit and monitor physical access to places when required for regulatory compliance. Physical access to these places must be controlled with badge readers or similar technologies.

When required for regulatory compliance, visitor logs and physical audit trails for access to Sensitive areas must be collected and kept in accordance with NSHE Records Retention and Disposition Schedule. All visitor access must be recorded in the *Visitor Log* (Appendix C.2).

Physical access to publicly accessible network jacks, wireless access points and payment processing terminals must be restricted, and ports must be disabled or otherwise secured from unauthorized access. Payment processing terminals are to be periodically inspected to look for tampering or substitution.

All networking equipment, communications hardware, and telecommunication lines must be physically protected.

Device consoles must be locked with user ID and password as per the appropriate System Configuration Guide.

### 3.4.1 Access to Sensitive Areas and Equipment

Access to Sensitive areas and equipment that may impact the overall security of the computing environment and network must be secured from unauthorized access. Areas deemed Sensitive will be protected with badge access systems.

For information on badge access requests and changes please contact UNR’s Facilities Services.

If a vendor, contractor, visitor or guest will be issued a badge with access to a Sensitive area, the request must be made, and Information Security notified at least 24 hours (1 business day) before the badge is issued.

### 3.4.2 Escorted Only Access

All employees without existing access, students, contractors, vendors, third-parties, and guests must obtain approval to enter high security areas. While accessing high security areas, employees without existing access, students, contractors, vendors, third-parties, and guests must be escorted by badged employees with access to the high security or restricted area. Regardless of affiliation, any person being escorted must fill out a visitor log. The escorting employee is to ensure they are with the person at all times and that all visitor logs are filled out per policy.

Students, contractors, vendors, third-parties, and guests issued a badge for identification purposes (not access purposes) must be stamped with a date of expiration that will revoke their access no longer than 24 hours (1 business day) from the date they are issued the badge.
3.4.3 Public Access Areas with Equipment Storing or Transmitting Confidential or Regulated Data

Any Users that will be using equipment storing or transmitting Confidential or Regulated Data in a non-secured area must wear proper identification that clearly identifies them as approved and affiliated with UNR to run and interact with the specified equipment. (E.g. students using mobile pay terminals on behalf of UNR programs should be clearly identified as allowed to be using mobile pay terminals, so that persons providing them with Regulated information required to process payments know they are providing the information to the correct person and not an imposter)

3.5 USER MANAGEMENT

3.5.1 Users

Every User must use a unique user ID and a personal secret password for access to UNR information systems and networks. All UNR systems housing Sensitive, Confidential, or Regulated Data must authenticate via password. This authentication will serve as a prerequisite to allowing access to organizational information systems. Shared or group user IDs are never permitted for user-level access to licensed, restricted or Sensitive resources. Shared or group user IDs may be used in a limited fashion for accessing wireless networks or general access workstations if a current University employee has been documented as the responsible party.

All Users must acknowledge understanding of the UNR Information Security policies by reading and acknowledging the Security Awareness and Acceptable Use Policy (Appendix A.1) prior to gaining access to UNR information systems and networks.

3.5.2 Terms of User Banner

All computer resources capable of displaying a terms of user banner should be configured as outlined in the appropriate System Configuration guide for the affected system.

3.5.3 Password Resets

Any unit or individual performing a password reset must first validate the identity of the user. The approved method of validation is either in person with a valid employee or government issued identification card, or remotely by verifying employee ID number, full name and date of birth, or application specific information that would only be reasonably known by the individual.

3.5.4 Contractor/Vendor Accounts

Contractor and Vendor accounts must have Information Security Department approval and must automatically expire at the end of the contract date. Extensions must be requested through Information Security. The responsible administrator or department must monitor these accounts carefully while they are in use.
4 IT CHANGE CONTROL POLICY

4.1 CHANGE MANAGEMENT

All UNR network devices, systems and application configurations will be subject to change management processes. Changes will follow the UNR change control process described in the Change Management Procedure (Appendix B.2) and the Minimum Change Process below. All changes will be approved, tracked, logged, and records kept in accordance with the Log and Data Retention Policy (Appendix A.2) and NSHE Records Retention and Disposition Schedule.

Exceptions to this section are applications owned by a specific department or unit in which the application is not enterprise level and the owner(s) will be responsible for all related user support.

4.2 MINIMUM CHANGE PROCESS

For all changes that meet the minimum requirement for formal change control, the responsible party that will be implementing the change must complete and submit a change request within the Information Technology Service Management System (ITSMS) to the approver of record. The change must be reviewed for approval, documented and if approved, scheduled. After approval and before or immediately after the change is complete, all applicable documentation must be updated. Please refer to the Change Management Procedure (Appendix B.2) for more information.

Requests must contain at a minimum the following information:

- **Impact Documentation** – The impact of the change must be documented so that all the affected parties (internal or external) will be able to plan accordingly for any processing change. In particular, all the systems, users and resources affected by the change must be documented and other service dependencies outlined. A start and end date and time must be provided.
- **Back-Out Procedures or Contingency Plan** – If the change does not go as intended a plan must be in place that describes the process of reverting the environment to its original configuration or other acceptable contingency plan outlined.
- **Test Plan** - A set of planned tests must be developed to verify that the change accomplished what it was supposed to do, and does not adversely affect other system components or create a weakness in the security posture of the environment. This plan may be specific to each change.
- **Management Approval** – All changes must include management approval.

4.3 CHANGE TESTING

Prior to introduction into the production network or systems all changes must first be tested on a QA or test network isolated from the production environment.

Testing of all security patches and system and software configuration changes must include, but is not limited to, the following:

- Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)
- Validation of proper error handling
- Validation of secure cryptographic storage
• Validation of secure communications
• Validation of proper role-based access control (RBAC)

The documented test plan must be followed to ensure no adverse effects on the network, systems or applications. Any discrepancies should be documented, and a new change request generated once all issues have been resolved.

4.4 CHANGE IMPLEMENTATION
All changes must be implemented according to the documented change procedures that were tested successfully. Any discrepancies between expected results and actual results that impact the network, systems, applications, business requirements or support procedures must result in the immediate invocation of the documented back out procedures.

4.5 EMERGENCY CHANGES
Certain events may require emergency changes that are exempt from the change control policy. Examples include, but are not limited to, unexpected service outage, security patches for vulnerabilities, and tasks related to onsite consultant activity.

In the event an immediate emergency change is required, an email must be sent to OIT managers and additionally to the IT alerts system when appropriate. The approval of two OIT managers is required prior to the emergency change being implemented.
5  DATA RETENTION AND DISPOSAL POLICY

5.1  RETENTION REQUIREMENTS
All systems will follow the NSHE Records Retention and Disposition Schedule.

Any additional retention or disposal requirements that differ from the NSHE Records Retention and Disposition Schedule must be (1) defined and justified within the system configuration guide as applicable to the affected system or process and (2) approved in accordance with Section 1 of the NSHE Records Retention and Disposition Schedule.

5.2  DISPOSAL REQUIREMENTS
All electronic and physical data and media, when no longer needed for legal, regulatory or business requirements, must be removed, made unreadable and unrecoverable, from UNR systems using an approved method documented in the NSHE Records Retention and Disposition Schedule and/or using industry best practice for secure deletion. This requirement includes all data stored in systems, temporary files, physical files, or contained on storage and backup media.

Programmatic (automatic) data disposal processes must be logged, reviewed and verified at least quarterly or as often as required to verify the process is working correctly and deleting data within the required time frame.

Media that will be reused or is part of shared storage space must be securely deleted using industry best practices that consider the media and data classification (sensitivity) as being wiped.

Hardcopy shred bins must remain locked at all times (until shredding occurs). Employees should make every effort to immediately cross-cut shred any printed material containing Sensitive, Confidential or Regulated Data.

Any additional disposal requirements defined by regulatory standards not previously covered in the aforementioned policies will be defined within the applicable system configuration guide(s) as applicable to the affected system or process.
6 PAPER AND ELECTRONIC MEDIA POLICIES

6.1 STORAGE

6.1.1 Physical Security

Hard copy materials and electronic media containing Sensitive, Confidential or Regulated Data must be protected by appropriate physical access controls as described in Section 3.4, Physical Security Policy.

6.1.2 Hardcopy Media

Hardcopy materials (e.g., paper receipts, paper reports, faxes, etc.) containing Sensitive, Confidential or Regulated Data are subject to the following storage guidelines:

At no time are printed reports of Sensitive, Confidential or Regulated Data to be removed from any UNR secure office environment.

Printed reports containing Sensitive, Confidential or Regulated Data must be physically retained, stored or archived only within secure UNR office environments, and only for the minimum time deemed necessary for their use.

At no time is printed material containing Sensitive, Confidential or Regulated Data to be removed from any UNR data center or computer room without prior authorization from Information Security.

When required for regulatory compliance, Regulated material must be sent or delivered by a secured courier or other delivery methods that can be accurately tracked and that have been approved by Information Security.

All hardcopy material containing Sensitive, Confidential or Regulated Data should be clearly labeled as such.

When required for regulatory compliance, all hardcopy media must be stored in a secure and locked container (e.g. locker, cabinet, desk, storage bin).

Sensitive, Confidential or Regulated hardcopy material is never to be stored in unlocked or insecure containers or open workspaces.

All University departments must shred all documents containing Regulated credit card information (PCI) in accordance with the shredding methods outlined in the NSHE Records Retention and Disposition Schedule and in compliance with the current applicable version of PCI compliance.

Other guidelines may be in place for protection of data and systems with additional regulatory requirements; those additional requirements will be defined in the system configuration guide(s) applicable to the system being protected and the data being processed.

6.1.3 Electronic Media

Electronic media (e.g., CD, DVD, floppy disk, hard disk, tape, USB “thumb” drive, etc.) containing Sensitive, Confidential or Regulated Data is subject to the following storage guidelines:
• When required for regulatory compliance, Regulated Data must never be copied onto removable media without authorization from Information Security.
• At no time is electronic media containing Sensitive, Confidential or Regulated Data to be removed from any UNR secure office environment with the exception of computer system backups.
• At no time is electronic media containing Sensitive, Confidential or Regulated Data to be removed from any UNR data center or computer room without prior authorization from Information Security.
• Electronic media containing consumer card data is to be physically retained, stored and/or archived only within secure UNR office environments, and only for the minimum time deemed necessary for their use.
• All electronic media containing Sensitive, Confidential or Regulated Data should be clearly labeled as such.
• All removable electronic media containing Sensitive, Confidential or Regulated Data must be stored securely.
• All media must be sent or delivered by a secured courier or other delivery methods that can be accurately tracked and that have been approved by Information Security.
• Use of portable storage devices with no identifiable owner is strictly prohibited where required by the regulatory environment.

6.2 INVENTORY
A Media Inventory Log (Appendix C.3) is to be kept in all secure media (hardcopy and electronic) storage locations when required by regulation. Any data including electronic and hardcopy media that must be stored securely will be inventoried and inventory lists reviewed and updated at least annually by the log owner.

Security controls and storage mechanisms will be reviewed yearly and verified during the inventory process. If discrepancies or deficiencies are discovered, they will be reported to the respective department heads and Information Security for review and remediation.

Some data types and systems will require additional processes for regulatory compliance; consult the appropriate system configuration guide(s) for more information.

6.3 DESTRUCTION
Hardcopy and electronic media must be destroyed as outlined in the NSHE Data Retention and Disposition Schedule.
7  SYSTEM CONFIGURATION, SECURITY AND ADMINISTRATION POLICY

7.1  DEVICE MANAGEMENT RESPONSIBILITIES
Management of all UNR devices (servers, routers, firewalls, workstations, Point of Sale (POS) machines, and other IT and/or PCI devices) shall be a combined effort of the IT Critical Systems Group, Network Operations and Information Security. Responsibilities of each group are defined in Roles and Responsibilities (Appendix D.1). Departments or units outside of OIT that manage their own computing resources must follow or request an exemption to this policy as described in Section 2 of the ISPP.

During the course of management of UNR devices, remote access of vendors, contractors or third-party support personnel may be required. All remote access of vendors, contractors or third-party support personnel must be supervised by staff during the entire remote session.

7.2  BASELINE CONFIGURATION
All systems, unless otherwise specified in their respective system configuration guide(s), will meet minimum industry best practices. UNR OIT will maintain a list of standards used with each system type within the systems configuration guides.

Any system that requires exemption from a known best practice requires a justification and approval from Information Security. Approval of the nonstandard configuration will be documented and reviewed at least annually.

Systems are, whenever possible, to be configured for a single purpose to ensure that mixed security requirements and levels are not present on the same system. (e.g.: web services and database services will not co-exist on the same sever.)

Systems must be configured to NOT use vendor-supplied defaults for system passwords and other security parameters. Defaults must be updated/changed to prevent unauthorized access.

During the configuration process, it is recommended for all systems that all unnecessary programs, functions, services, ports, and protocols be disabled. This is mandatory for all systems containing Sensitive, Confidential, or Regulated Data.

All installed software and configurations must be approved by the appropriate party. Where applicable and when required by regulatory compliance, an inventory of systems and installed software will be required and must be kept in the system configuration guide or appropriate log.

Service owners shall maintain an access control list identifying all authorized users to systems and applications that store Regulated Data, along with their access rights assigned to them.

Access restrictions must be in place to allow only approved individuals to make physical or logical changes when required on UNR’s information systems. Physical and logical changes must be documented in the approved change management system along with the authorized employee that made the changes.
A deny-by-exception (blacklist) policy will be applied to prevent the use of unauthorized software in environments containing Regulated Data. Additionally, when applicable, a permit-by-exception (whitelist) policy will be applied to allow the execution of authorized software.

New and repurposed systems must be configured according to the device type, security level, and in accordance with the system configuration guide that most accurately represents the requirements and data stored or processed by the system. If the data type, security levels, and/or regulatory requirements are new to the organization, either an update to existing, or creation of new system configuration guide(s), will be required.

All systems will be evaluated for proper configuration, including the latest security patches and comparisons to the system configuration guide(s), before being placed into the live production environment.

Appropriate steps must be taken to prevent remote devices from simultaneously establishing non-remote connections with information systems containing Regulated Data and communicating via some other connection to resources in external networks. Remote activation of collaborative computing devices is strictly prohibited in environments containing Regulated Data. Furthermore, indication of devices in use is provided to users present at the device.

7.3 CONFIGURATION CHANGES, UPDATES AND PATCHES
Changes to base configuration will be reflected in System Configuration Guide(s). System Configuration Guides will be reviewed at least annually unless otherwise specified within the guide for regulatory compliance.

Critical and security updates are implied as a base configuration requirement. All systems will have all critical security patches installed in a timely manner consistent with industry best practice and do not require an update to the system configuration guide documents.

A log of system changes and updates including patches may be required for certain regulatory compliance standards. The systems adhering to those standards will be identified in the System Configuration Guides.

Where applicable, adherence to change management may be required. Administrators should consult the Change Management Procedure (Appendix B.2) for more information.

7.4 SECURITY VULNERABILITY & NETWORK SCANNING
All vulnerability and network scanning must be approved by Information Security before the scanning is to take place. At no time shall any person, department, or entity scan the UNR network without prior written authorization from Information Security. Information Security reserves the right to validate both the process of scanning, and any results from scanning, using industry accepted best practices.

Information Security will perform internal vulnerability and network scanning to troubleshoot, investigate, and otherwise manage the UNR network. Any files downloaded, opened, or executed from external sources will have real-time scans performed to check for the presence of malicious code.
Scanning will be done as needed for general networks and as outlined in the System Configuration Guides for all other instances and requirements. External vulnerability scanning will be performed regularly, and all scans will be performed by qualified scanners.

If vulnerability scans uncover potential vulnerabilities, Information Security personnel must be notified so remediation efforts may begin. Personnel must follow the Change Control Policy (Section 4) to correct high-level vulnerabilities. Additional scans must be performed in order to confirm compliance with UNR OIT security standards.

For external networks that have additional regulatory compliance standards, the additional requirements will be defined in the System Configuration Guide(s) for those networks and systems.

All scan processes and results are to be considered Confidential and protected appropriately.

7.5 RISK ASSESSMENTS
On an annual basis, a formal risk assessment will be conducted by UNR OIT on certain systems to ensure UNR’s data assets are being sufficiently protected. This assessment will identify any existing or new vulnerabilities in specified systems. The ISPP along with other applicable documents will be updated as necessary to reflect any findings from the risk assessment. A plan of action will be maintained to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.

7.6 SECURITY CONTROL ENFORCEMENT
No one shall implement systems or create configurations that are meant to bypass or circumvent any University security control. This includes, but is not limited to, hiding or obfuscating network traffic through a firewall using encryption or alternate ports, creating Virtual Private Networks (VPN) to tunnel traffic to or through the University’s network, impersonating another device, or embedding inappropriate content in encrypted files for the purpose of bypassing anti-malware systems. An exception may be granted in certain circumstances for VPNs if a legitimate business need is presented and no other alternatives are available.

7.7 LOGS
All systems that require logging will have logging enabled. Logs will be kept in accordance with the Log and Data Retention Policy (Appendix A.2) and the NSHE Records Retention and Disposition Schedule and/or based on regulatory requirements of that particular system. The System Configuration Guides will define additional logging requirements as needed.

As a baseline, any system logging should log at a minimum enough information to identify users, system login, data accessed, administrative functions, and unsuccessful attempts at access.

Systems will also log as follows:

- Systems defined as Unrestricted – Logging is recommended to be enabled whenever possible. Logging should only be disabled when it is resource prohibitive and approved by Information Security.
- Systems defined as Sensitive or Confidential – Logging is to be enabled. Additional logging
requirements will be specified in the system configuration guide as appropriate.

• Systems defined as Regulated – Logging is to be enabled. Log forwarding to Security Information and Event Management (SIEM) or other secure logging practices are required. Additional logging requirements will be specified in the system configuration guide as appropriate.

7.8 AUDIT & ACCOUNTABILITY

Audit and event logs must be regularly reviewed and updated by assigned personnel. Where a manual review of the logs is not feasible, the central logging system must be configured to alert and report on auditable events as identified by the Information Security Department. Security monitoring systems must be configured to alert in the event of suspicious activity. The Information Security Department will correlate audit review, analysis, and reporting processing for investigation and response to indications of inappropriate, suspicious, or unusual activity. Alerts are to be sent to the Information Security Department and responded to in accordance with the Incident Response policy. In the event that an audit process fails, an alert must be in place notifying the Information Security Department.

Correct, accurate, and consistent time on all UNR system components must be maintained. Time signals at UNR are required from UNR time servers, which is an industry accepted external source based on Coordinated Universal Time (UTC). Network Time Protocol (NTP) is utilized by UNR. All UNR production systems, with the exception of UNR’s internal NTP servers, must be configured to utilize the internal NTP server for time synchronization purposes. Access control lists must be configured to limit access to the time setting of UNR’s NTP server. The internal NTP server must be running a supported version at all times.

UNR utilizes a centrally managed Security Information Event Management System as its logging and auditing solution. This service is to be restricted to personnel with business need to know by way of access control lists to prevent unauthorized manipulation of this tool and its function.

All audit logs for systems that store Regulated Data are to be stored on a centralized log server to ensure the logs are secure from unauthorized access or modifications. The logs will only be accessed and viewed on a “need to know” basis. The Information Security Department must establish a file integrity monitoring (FIM) system that will alert personnel in the event either unauthorized access to logs or modification of logs occurs. Logs must be retained in accordance with the Log and Data Retention Policy (Appendix A.2).

7.9 MAINTENANCE

Restrictions will be put in place to limit the tools, techniques, mechanisms, and other personnel used to conduct information system maintenance. Any equipment that is removed for off-site maintenance is to be sanitized of any Regulated Data. Prior to use in the information system, any media containing diagnostic and test programs may be required to be tested for malicious code depending on the regulatory environment. Non-local maintenance sessions are not permitted on UNR systems.
8    ELECTRONIC MEDIA BACKUP POLICY

8.1   LOCATION
The backup media for systems containing Sensitive, Confidential or Regulated Data should be replicated or relocated to a secure off-site storage area.

All hosted off-site storage locations must be visited annually by management or a member of Information Security or their designee to confirm that it is physically secure when required for regulatory compliance.

Cloud-based backup systems may be used so long as the service/location has and is using industry accepted strong encryption to protect the data in transit and at rest on the cloud service servers.

8.2   TRANSPORT
Offline storage media utilized for archival or back-up purposes must be handled and retained in a secured environment such that only UNR personnel and contracted storage facility personnel have access to the archival media.

All media couriers and transport mechanisms must be approved by Information Security.

Positive log-out and log-in of archive media will take place during all archive media transfers when required by regulation. All media that is transferred from one location to another should be logged as being transferred, by whom, where, and whether properly received, with signature from a management approved designee. The Backup Media Transfer Log (Appendix C.4) must be used to document this process.

All media containing Sensitive, Confidential or Regulated Data must be classified and identifiable as such prior to transfer as detailed in the Data Classification and Control Policy (Section 3).

Due to the nature of cloud-based backup, no transport of physical media is expected; however, if seed drives (preloaded backup drives) are used, they must be transferred in a secure manner with delivery tracking, and with encryption. Over-the-wire (internet, VPN, etc.) transmissions to cloud systems require a secure method with encryption applied to the data being backed up.

8.3   AUDIT
All media used will be classified as Sensitive, Confidential or Regulated and assigned a unique tracking number or similar feature that uniquely identifies the media. All media from critical systems must be registered with Information Security or IT Critical Systems Group for tracking prior to use.

Quarterly inventories of all stored media will take place when required by regulation. Information Security will compare their list of in-use media with records at the storage facility using the Media Inventory Log (Appendix C.3).
8.4 MEDIA DESTRUCTION

All media that is no longer needed or has reached end-of-life must be destroyed or rendered unreadable so that no data may be extracted. Information on acceptable destruction techniques is detailed in the Data Retention and Disposal Policy (Section 5).

For cloud-based systems a certificate of secure deletion and/or destruction from the provider is required to ensure confidentiality of the data.
# 9 ENCRYPTION POLICY

## 9.1 GENERAL ENCRYPTION REQUIREMENTS

Whenever data is Sensitive, Confidential or Regulated, data is to be encrypted in transit. Data may also be required to be encrypted at rest, depending upon the data (see System Configuration Guidelines).

Appropriate encryption methods are to be invoked for such media containing Sensitive, Confidential or Regulated Data when stored on backup media. When feasible, encryption controls should be implemented to ensure the media itself is encrypted and protected from unauthorized access.

Encryption will be based upon industry standard strong encryption (See NIST Cryptographic Toolkit, which provides standards and guidance covering a wide range of cryptographic technology and can be found on the NIST website here: [http://csrc.nist.gov/groups/ST/toolkit/](http://csrc.nist.gov/groups/ST/toolkit/)).

FIPS-validated cryptography with a minimum block size of 128 bits and a minimum key size of 256 bits will be used to protect data containing Regulated Data.

Authentication credentials must be encrypted, and all authentication (of a system or user) must be done securely and via an industry standard method of encryption. UNR’s approved encryption protocols are to be utilized when accessing system components. Passwords stored in databases, access control systems, files, etc. must be encrypted while at rest. Credentials passed from one system to another must never pass in clear text or be reversible by a third party.

Full disk encryption and pre-boot encryption in use in various applications is defined in the System Configuration Guides for each particular system.

Transmission of encryption keys (crypto keys) over untrusted networks will be encrypted with industry standard encryption. The encryption used to encrypt the crypto keys to be transmitted must be encrypted with a different key than the keys being exchanged.

Key management, knowledge & dual control, generation, distribution, storage, and destruction are all elements specific to the systems and data sets in question and will be addressed as needed in the System Configuration Guides.

If any crypto key set is thought to be compromised the key will be retired and relevant data re-encrypted with a new uncompromised key.

In the event an encryption methodology, algorithm, or process is broken or compromised, all affected systems are to be evaluated, and a remediation plan put into place to update, patch, or replace the broken methodology or algorithm within a reasonable time frame.

## 9.2 TRANSMISSION OVER UNTRUSTED NETWORKS

Sensitive, Confidential or Regulated Data must be encrypted during transmission over untrusted networks in which it is easy and common for the data to be intercepted, modified or diverted using industry-supported strong encryption protocol. Untrusted networks include unencrypted guest
9.3 ENCRYPTION OF WIRELESS NETWORKS

All wireless networks in use at UNR facilities must be protected through secure data encryption such as Wi-Fi Protected Access II (WPA2) or higher or TLS 1.2 or higher. Under no circumstances should the encryption strength be configured to be less than 128 bits. WEP is a vulnerable technology and must never be used to protect wireless networks within the PCI cardholder environment. Wireless networks, such as WPA2, utilize authentication on a user level. To provide a secure wireless network for enterprise use, users must login with their NetID and password for authentication. The Information Security Department manages signed certificates via Incommon to protect communication sessions.

Guest wireless networks without encryption are allowed but must be restricted by a secure portal authentication system and only allow VPN or HTTP/HTTPS traffic. Guest network access accounts must be documented in the ITSMS. No guest wireless access is allowed within the cardholder environment.

9.4 EMAIL TRANSMISSION OF SENSITIVE, CONFIDENTIAL OR REGULATED DATA

Sensitive, Confidential and Regulated Data is never to be sent unencrypted through end-user messaging technologies such as e-mail, instant messaging, or chat.
10 SOFTWARE DEVELOPMENT POLICY

10.1 SOFTWARE DEVELOPMENT: GENERAL USE DATA
In the event OIT develops software for Unrestricted Data, all applicable industry best practices will be followed as best suited for the development of the software.

OIT does not consider scripts or other automated tasks as software development; however, OIT will still thoroughly test and review the scripts and automated tasks for potential security issues.

10.2 SOFTWARE DEVELOPMENT: SENSITIVE OR CONFIDENTIAL DATA
All development of software for Sensitive or Confidential Data processes or systems will adhere to the following requirements:

A test/development environment, separate from the production environment, must be used to test all new software (including patches). If the network has network connectivity to the production UNR network, access controls must be in place to enforce the separation.

Production data will not be used for testing and development purposes without being sanitized. Test personnel should make every effort to use mock data only for testing on non-production systems and software.

All test data and test accounts must be removed before a system goes into production. Similarly, all custom application accounts, user IDs and passwords must be removed before an application goes into production or is released to end users.

10.2.1 Development Life-Cycle
Internal and 3rd party development of proprietary software must utilize industry recognized best practices for software development. Security checks and control measures must be considered throughout the development life-cycle.

The high-level overview of the security measures taking place within each phase of the UNR development process are as follows:

- **Requirements Analysis** – Developers should determine whether application requirements are inherently insecure.
- **Design** – Application components must be planned in a manner consistent with data and network security.
- **Development** – Developers must consider all application vulnerabilities (i.e.: memory bound issues, privilege and access bypass, etc.).
- **Documentation** – All application feature and implementation documentation must include direction on proper security configurations.
- **Production Implementation** – Implementation must not compromise security controls already in place or introduce new vulnerabilities.
- **Production Testing** – In addition to functional and efficiency testing, all security features of the application must be tested.
- **Maintenance** – All future application maintenance should not compromise security controls
already in place or introduce new vulnerabilities. Any new code must be reviewed and tested as detailed above.

10.2.2 Web-based Applications
In addition to all the security measures that take place throughout the application development life-cycle, special care should be given to UNR applications that are web-based.

All development must occur taking the Open Web Application Security Project (OWASP) guidelines into account. These guidelines are available at https://www.owasp.org. Specifically, the following vulnerabilities must be considered during the Code Review and Testing phases:

- Data Validation
- Authentication
- Session Management
- Authorization
- Cryptography
- Error Handling
- Logging
- Security Configuration
- Network Architecture

Note: The vulnerabilities listed above were the current ones in the OWASP guide when this policy was released. However, if and when the OWASP guide is updated, the most current version will apply. Software development should always occur with reference to the most recent guidance from OWASP and other respected outside sources.

10.3 SOFTWARE DEVELOPMENT: REGULATED DATA
OIT will not develop software for any Regulated Data processes or systems.

In the event a UNR entity develops software for Regulated Data processes or systems, that entity is responsible for following all related regulatory compliance.
11 INCIDENT RESPONSE PLAN AND PROCEDURES

11.1 INCIDENT RESPONSE REQUIREMENTS AND INFORMATION
UNR will maintain an Incident Response Plan. The Incident Response Plan will be reviewed at least annually and after any activation of the Incident Response Plan (See Appendix E.1). Information Security reserves the right to bill back actual costs incurred in responding to incidents to the unit responsible when appropriate.

On an annual basis, the current Incident Response Plan will be tested by means of a “mock incident”. The Information Security Department will facilitate and plan the incident at their discretion. All procedures outlined in the Incident Response Plan (See Appendix E.1) must be followed. This test will involve any and all UNR employees who have an active role in the Incident Response Plan.

Any suspected, perceived or known incident is to be reported to Information Security immediately.

11.2 BUSINESS CONTINUITY PLANS
Each University unit that provides critical IT infrastructure is responsible for outlining their business continuity policies and procedures specific to their individual requirements.

11.3 AUTOMATED SECURITY SYSTEM NOTIFICATIONS
All automated intrusion detection systems within the UNR Sensitive, Confidential or Regulated environments, including intrusion detection sensors and file integrity checking systems, will be configured to automatically notify Information Security of any potential compromises or attacks. Also, any automatic or manual detection of unauthorized wireless access points must trigger the Incident Response Plan.

Information Security will extend best efforts to provide 24/7 availability to initiate the Incident Response Plan if warranted.
12 THIRD PARTIES AND THIRD PARTY AGREEMENTS

12.1 UNRESTRICTED DATA AGREEMENTS
UNR may at times be required to share data with other entities. When the data being shared is beyond the scope of public records, UNR may require at the discretion of NSHE, legal counsel, data governance boards, and data owners, a third-party agreement or contract.

When such agreements are required, the agreement terms must be declared and fully executed by individuals with appropriate signature authority before any data is shared.

When required for regulatory compliance, a list of all third parties with whom data is shared will be maintained and updated on a regular basis by the data owner or their designee.

12.2 SENSITIVE, CONFIDENTIAL OR REGULATED DATA AGREEMENTS
UNR may at times be required to share Sensitive, Confidential or Regulated information (proprietary, PII, PCI, HIPAA, etc.) with third parties. UNR will require at the discretion of NSHE, legal counsel, data governance boards, and data owners, contractual or business associate agreements (BAA’s) with those third-parties that will, at a minimum, define the protections required to maintain the security and sensitivity of the data being shared. The only time an agreement is not required is when the data falls under a regulatory control that explicitly authorizes transfers of the data without an agreement.

Agreements must be fully executed by individuals with appropriate signature authority before any data is shared.
This page is intentionally blank to indicate the end of this document.