BURRELL COLLEGE OF OSTEOPATHIC MEDICINE

STANDARD OPERATING PROCEDURES

Information Security Plan	SOP #: IT.006.02
Effective Date	12.9.19
Last Revision/Review	9/15/2022

1. Purpose

a) In order to protect privacy and personal information of Burrell stakeholders, Burrell College of Osteopathic Medicine (Burrell) has developed a Written Information Security Program (WISP). This is a comprehensive set of guidelines that have been implemented in compliance with federal, state and international regulations and standards. The goal of this plan is:

   a. To insure the security and confidentiality of stakeholder information
   b. To protect against any anticipated threats to the security or integrity of such information
   c. To guard against the unauthorized access to, or use of, such information that could result in substantial harm or inconvenience to any stakeholder.

2. Related Policy/Authority

a) Burrell Policy B2050 – Data Security Policy
b) Burrell Policy B2090 – Records Retention
c) Federal Student Aid Office - CPA-19-01, Amendment to September 2016 Audit Guide, *Guide for Audits of Proprietary Schools and For Compliance Attestation Engagements of Third-Party Servicers Administering Title IV Programs* – Student Information Security
d) NIST-800-171 – *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
e) Gramm–Leach–Bliley Act (GLBA), , (Pub.L. 106–102, 113 Stat. 1338)

3. Faculty/Staff Responsibilities

a) The office of the Chief Information Officer is in charge of maintaining, updating and implementing this plan.
b) Individual departments are responsible for implementing and insuring compliance with all applicable College policies and procedures. See Records Retention Policy B2090 and Records Retention Standard Operating Procedure for Data Custodian assignments.

4. Definitions/Abbreviations

a) NIST – National Institute of Standards and Technology
b) GLBA – Graham Leach Bliley Act
c) FERPA – Federal Educational Privacy Rights Act
d) PII – Personally Identifiable Information
e) CUI – Controlled Unclassified Information. For purposes of this document, PII and CUI may be used interchangeably.
f) ACH – Automated Clearing House electronic payment
g) MFA -- Multi Factor Authentication

5. Procedural Steps

This procedure describes steps to insure data security and integrity at Burrell. It is written to conform to the NIST-800-171 standard for the protection of Controlled Unclassified Information (CUI). References to relevant NIST standards are provided as appropriate.

The Data Integrity Committee will prepare an annual report of activity, including mitigated risks and outstanding issues for future mitigation.

a) Access Control (NIST 800-171-3.1)
   a. Burrell employees, contractors, and others are granted access to the minimal set of data for them to execute their job functions. Access to systems and services are authorized by an employee's supervisor based on need.
   b. All employees are responsible for maintaining the privacy and integrity of PII and CUI.
   c. Any computer file containing personal information will be kept password-protected, and utilize a screen locking tool when unattended.
   d. When there is a need to bring records containing CUI off-site, only the minimum information necessary will be brought;
   e. Records brought off-site should be returned to the Burrell as soon as possible.
   f. Under no circumstances are documents, electronic devices, or digital media to be left unattended in an employee's car, home, or in any other potentially insecure location.
   g. Any laptop or portable device which has personal information stored on it will be kept encrypted using a whole-disk or whole-device encryption solution at all times.
   h. No personal information is to be disclosed without first fully authenticating the receiving party.

b) Awareness and Training (NIST 800-171-3.2)
   a. All Burrell employees receive training on FERPA, GLBA, data security, and data responsibility as a part of the on-boarding process.
   b. Burrell employees receive refresher training on these topics annually.
   c. All employees must read and sign the "Non-Disclosure / Acceptable Use Agreement"

c) Audit and Accountability (NIST 800-171-3.3)
   a. All user accounts will be unique, and will be password protected. Account information is not to be shared.
   b. Business systems will have logging enabled to allow monitoring of activity to insure appropriate use pursuant to Burrell Data Security Policy B2050.

d) Configuration Management (NIST 800-171-3.4)
   a. All hardware and software purchases are coordinated through the Information Technology (IT) department.
   b. Prior to distribution to end users, all hardware systems are configured by the IT department to include centrally managed virus and malware protection as well as patch management.

  c. All servers and systems, including system interfaces, system input portals and system report distribution, are regularly updated for security patches.

e) Identification and Authentication (NIST 800-171-3.5)
  a. All Burrell users are required to use their personal passwords to access any Burrell system. Shared login credentials are not permitted.
  b. All credentials are managed and authenticated on a centrally controlled system.
  c. Multi factor authentication is required for certain types of system access. It is available optionally for all users.
  d. Passwords must adhere to complexity standards. Passwords are managed per NIST 800-63 password guidelines.

f) Incident Response (NIST 800-171-3.6)
  a. Any suspected data breach should be reported immediately to the Chief Information Officer (CIO). While an initial report may be verbal for expediency, a written report should be filed as soon as practical.
  b. Burrell's CIO will thoroughly document and review any breach that may occur.
  c. Any suspected breach shall be evaluated for severity and scope.
  d. The CIO will be responsible for reporting all breaches or other significant events to appropriate entities, which may include the Burrell Executive Management, Burrell Board, Federal, State, and regulatory agencies.
  e. The CIO shall be responsible for insuring any affected individuals are notified of a breach that may affect them as required by law or regulation.

g) Maintenance (NIST 800-171-3.7)
  a. All Burrell computer hardware requiring service will be coordinated through the IT department.
  b. The IT department shall insure that no CUI is present on any system returned to a manufacturer or vendor for service.

h) Media Protection (NIST 800-171-3.8)
  a. All CUI stored electronically shall be kept on centrally controlled systems.
  b. Physical access to servers in the Burrell data center is controlled via keycard, and monitored by security cameras.
  c. Any devices containing CUI will have hard drives removed, or be scrubbed with approved data protection tools prior to disposal.
  d. When disposing of paper records, a crosscut shredder or a certified shredding service will be used.
  e. Physical repositories for records containing CUI may include file cabinets, document storage facilities, and/or document storage services. These shall be located in access restricted areas, and locked. A complete inventory of all these repositories shall be reviewed regularly, with a formal inventory at least annually.
  f. Paper records will be kept behind lock and key.

i) Personnel Security (NIST 800-171-3.9)

a. All employees must read and sign the "Non-Disclosure / Acceptable Use Agreement"

b. Any employee who either willfully or through gross negligence discloses personal information or fails to comply with these policies will face immediate disciplinary action up to and including the possibility of termination. A failure of an employee to appropriately manage PII will be addressed per Burrell policy and procedures.

c. Any terminated employees' computer access passwords will be disabled before the employee is terminated. Physical access to any documents or resources containing personal information will also be immediately discontinued. Burrell reserves the right to temporarily suspend employee access at any time to documents and systems if in the best interests of Burrell.

d. Automated systems shall be used to automatically remove or disable accounts and system access upon employee separation where possible.

e. During employee off-boarding, a checklist verifying access has been terminated shall be kept.

j) Physical Protection (NIST 800-171-3.10)

a. The entire Burrell facility is normally kept locked, with access for students and staff granted via keycard.

b. The on campus data centers have restricted access, which is controlled via key card.

c. The keycard system provides logging for all building access, including failed access attempts.

d. Visitors are required to check in with security, and be escorted to appointments.

k) Risk Assessment (NIST 800-171-3.11)

a. The type of records that are collected and maintained by Burrell, and where and how they are stored shall be reviewed regularly, with a formal inventory at least annually.

b. Electronic repositories for records may include local or remote servers; workstations; backup devices or services; or 3rd party software / hardware / service platforms. A complete inventory of all these repositories shall be reviewed regularly, with a formal inventory at least annually.

c. In conjunction with the Continuity of Operations Plan (FAC-010) – the impact of severe operational disruption shall be assessed annually, with recommendations for mitigation or remediation.

d. In accordance with the Records Retention Policy (B2090), records will be disposed of as required to reduce the liability of keeping unneeded CUI.

e. Penetration testing shall be performed regularly, with a remediation action plan drafted for issues that are discovered.

l) Security Assessment (NIST 800-171-3.12)

a. User accounts and permissions shall be reviewed periodically to insure appropriate access.

b. Any identified deficiencies with respect to this plan shall be documented, with a remediation / mitigation path defined.

   c. As appropriate, electronic tools and techniques may be employed to test existing electronic safeguards. This may include penetration testing, social engineering vulnerabilities, etc.
   d. Security audits shall be performed annually.

m) System and Communication Protection (NIST 800-171-3.13)
   a. All points where private Burrell networks touch public or non-Burrell networks shall be protected by firewalls.
   b. Firewalls shall be configured to specifically permit desired traffic by exception, and to reject everything else.
   c. Internal clients and services are segregated to different virtual networks, with cross network traffic controlled by access control lists.
   d. Network shall be designed to only allow the minimum access level needed by job function for different classes of users.
   e. Firewalls and other security related systems shall be configured to provide active alerting in the event issues are found.
   f. All systems and endpoints will have current, centrally managed virus and malware protection.
   g. All external system communications shall employ VPN encryption.

n) System and Information Integrity (NIST 800-171-3.14)
   a. All trouble / security alerts are to be investigated by the Burrell IT office, or 3rd party security management provider.
   b. Any significant issues that are found are to be entered as a trackable work order so that resolution can be documented.
   c. All systems are to be routinely audited for compliance with industry best practice and Burrell operational standards.
   d. Burrell will conduct regular network security audits in which all server and computer system logs are evaluated for any possible electronic security breach. These audits will be performed as appropriate but at a minimum every 30 days.

6. Reports/Charts/Forms/Attachments/Cross References

SOP FAC.010 – Continuity of Operations

7. Maintenance

a) This plan is reviewed periodically and amended as necessary to protect personal information. It is formally reviewed at least annually.

8. Signature

Approved by	9/15/2022
Chief Information Officer	Date

9. Distribution List

Internal/External

10. Revision History

Revision Date	Subsection #	Summary of Changes	New/Cancellation/ Replacement Procedure? (if applicable)	Approval Date
2021-12-01	All	Fixed typographical errors		12.2.2021
9/15/2022	All	Added information about Data Integrity Committee		9/15/2022