UNIVERSITY of HOUSTON SYSTEM

INFORMATION SECURITY

Level 1 Data Protection Requirements Checklist (per SAM 07.A.08)

All Level 1 Data must:

- ☐ Be stored on a critical information resource. See separate checklist below.
- ☐ Have appropriate data access controls in place.
  - ☐ Access must be granted only through the use of individual user ID accounts with complex passwords (SAM 07.A.10).
  - ☐ User groups based on roles or level of access.
  - ☐ Shared or departmental accounts are not permitted (SAM 07.A.10).
  - ☐ Periodic audit of access list of user accounts.
- ☐ Not be transmitted via wireless network devices unless encrypted.
- ☐ Not be transmitted by e-mail unless encrypted.
- ☐ Be encrypted at rest when technically and feasibly possible.
- ☐ Not be stored on a removable or portable device such as a flash drive, tablet or laptop. If a valid business need requires Level 1 data to be stored on a removable or portable device, the information must be encrypted.
- ☐ Not be stored on non-university devices. If a valid business need requires level 1 data to be stored on a non-university device, specific permission must be obtained in advance from the department/unit head or component University Information Security Officer.

Critical Information Resource Requirements Checklist (per SAM 07.A.08)

All university critical information resources must have:

- ☐ Physical access granted only to authorized personnel via access cards, keys or other control mechanisms.
- ☐ Environmental systems with monitoring to ensure protection from environmental hazards.
  - ☐ Adequate HVAC and ventilation.
  - ☐ Fire prevention and suppression.
  - ☐ Flood or water protection.
- ☐ Regularly completed backups of all data and the backup data stored in a separate, secure area.
- ☐ Uninterrupted power supply (UPS).
- ☐ Relevant security patches installed.
- ☐ Anti-virus software installed and appropriately configured and managed by a group console for verification, like McAfee ePO.
- ☐ Unnecessary and/or inactive system or appliance accounts must be disabled or deleted.
- ☐ Vendor-supplied system passwords replaced with strong passwords.
- ☐ Audit/security logs enabled.
- ☐ Prior to the disposal of the critical information resource, a secure destruction method must be used to ensure the resource is sanitized rendering the data unrecoverable.

*The above checklists for are based on the University of Houston System Administrative Memorandum (SAM) 07.A.08, Data Classification and Protection, requirements for the protection of Level 1 data. Requirements for other compliance frameworks, such as FERPA, HIPAA, PCI, GDPR, or DMCA must be adhered to in addition to the SAM requirements.