ISO Policy Compliance Guidance

Purpose of Document

This document provides guidance to University colleges, units, and programs (hereafter referred to as "units" for brevity) on a comprehensive recommended framework for achieving compliance with requirements contained in Information Security Office (hereafter referred to as ISO) Policies published on https://security.arizona.edu/content/policy-and-guidance.

Units should use this document to ensure that each requirement is met for a given area or system. An area could be as broad as an entire department or as narrow as a single research project. Similarly, systems may range from enterprise systems to something extremely narrow such as document storage for a single user.

Requirements are grouped into three sections: administrative, technical and physical. Each section may contain up to three groups of subsections that further clarify the exact requirements needed to satisfy the parent section or subsection. For convenience, the comprehensive list of ISO Policy requirements has been included in this document's appendix.

ISO Policy requirements may be satisfied in a manner other than the recommended framework detailed in this document. The ISO is committed to providing solutions that enable ISO Policy compliance and make compliance reporting easy. However, business requirements in a specific unit may necessitate the implementation of alternate solutions to satisfy ISO Policy compliance and/or manual compliance reporting.

1. Administrative Requirements

1.1 UA ISO Policies are well understood and easily accessible to the impacted workforce. Workforce must know about and be able to find: https://security.arizona.edu/content/policy-and-guidance.

1.2 Workforce has received required information security, privacy, regulatory, and role-based training. This includes, at minimum, the mandatory annual Security Awareness Training and refresher course. Refer to the Information Security and Privacy Training standard and check with relevant information security and privacy compliance offices (https://compliance.arizona.edu/compliance-partners) for additional training requirements.

1.3 Information security roles are assigned and communicated to the workforce and to UA ISO. The ISO has defined specific security roles. Each unit must designate persons to fill these roles:
(1.3.1) Information Resource Owner(s) (Information Owners and Information System Owners) – the role with authority and accountability for enabling implementation of information security controls.
(1.3.2) IT Security Manager(s) – the role responsible for implementing information security controls in a manner consistent with the information security plans for an information resource.
(1.3.3) Information Security Risk Manager(s) – the role responsible for coordinating people and activities to complete the information security risk management process and in creating the information security plan for an information resource.

1.4 Unit procedures are aligned with UA ISO Policy, formally documented, and implemented and communicated to the workforce and to UA ISO. Unit must ensure procedures satisfy ISO Policy minimum requirements. Alignment may be achieved by adopting default ISO processes and limiting tailoring of procedures as indicated in the corresponding guidance for ISO process documents. Procedure alignment and implementation must ensure:
(1.4.1) Unit information security and privacy procedures are defined and documented. Unit must ensure procedures are documented in a location that is accessible to the workforce and the ISO. The documented procedures must include: (1.4.1.1) Risk management and security planning procedures, (1.4.1.2) Information security and privacy audit response procedures, (1.4.1.3) IT Asset inventory procedures, (1.4.1.4) Information security and privacy event reporting procedures, (1.4.1.5) Access control determination and review procedures – physical and technical – user and administrator, (1.4.1.6) Supervision procedures for persons who work in areas where Confidential and/or Regulated data is accessible but who have not met the 'need to know' threshold, (1.4.1.7) Patch management procedures, (1.4.1.8) Vulnerability management procedures, (1.4.1.9) Physical access control procedures, (1.4.1.10) Workforce termination procedures, (1.4.1.11) Hardware and software license compliance assurance procedures, (1.4.1.12) Architecture and engineering procedures – architectural review, secure coding, etc., (1.4.1.13) Device hardening procedures, and (1.4.1.14) Activity report review procedures.
(1.4.2) Workforce members are trained on and implement information security and privacy procedures. Unit must ensure workforce can find and utilizes documented security and privacy procedures.

1.5 Unit information security and privacy practices are established and enforced. Unit must ensure security and privacy practices support their business requirements. The practices must ensure:
(1.5.1) Unit information security and privacy practices are determined and documented. The documented practices must include: (1.5.1.1) Role based information security and privacy training requirements, (1.5.1.2) Periodicity and method(s) of compliance evaluation, (1.5.1.3) Methods of vendor and contract review and management, (1.5.1.4) Permitted use of removable media, (1.5.1.5) Required end user device protection and permitted Bring Your Own Device (BYOD) practices, and (1.5.1.6) Information retention and disposal practices.
(1.5.2) Workforce members incorporate information security and privacy practices into their business processes. Unit must observe workforce to confirm that security and privacy practices are being followed.
(1.5.3) MOUs, SLAs, EULAs, and other agreements entered into with customers describe relevant information security and privacy practices. Unit must document any deviation from ISO Policy and the separation of security and privacy responsibilities between the unit and other University stakeholders.
(1.5.4) Vendor agreements are reviewed to confirm compliance with UA ISO Policy and Unit practices. Unit must review contracts to either negotiate the inclusion of or make alternative mitigations to satisfy information security contract requirements: https://confluence.arizona.edu/display/UAIS/Information+Security+Contract+Language.

1.6 Third party and regulatory information security and privacy requirements are met. Unit must document compliance with any applicable third party and regulatory requirements. Meeting requirements includes:
(1.6.1) Information resources are assessed, in collaboration with UA ISO and compliance

offices, to determine regulatory implications.
(1.6.2) Information security and privacy practices are reviewed and approved by appropriate compliance offices: https://compliance.arizona.edu.
(1.6.3) Information security and privacy practices are assessed against contracts and agreements, such as DTAs/DUAs, that impose requirements on the unit.

1.7 Information resources are identified and managed. Unit must participate in the ISO Information Security Risk Management program. Participation must include:
(1.7.1) IT Assets are inventoried and characterized according to system criticality and information classification. ISRM must update the inventory of all unit IT Assets at least annually.
(1.7.2) Information, data, collections, etc. are identified, inventoried, and classified according to UA Data Classification Standard. ISRM must categorize IT Asset Inventory using the following standard: https://security.arizona.edu/content/data-classification-and-handling-standard

1.8 For systems containing confidential and/or regulated information and systems considered critical to the business, contingency access and data protection planning has been performed. Unit must document and perform periodic testing on a contingency plan for all confidential and/or regulated information systems and systems considered critical to the business using an ISO approved or substantially equivalent template. Contingency plans must meet the following requirements:
(1.8.1) A contingency access plan has been developed and documented. Unit contingency plans must document contingency access.
(1.8.2) A data backup plan has been developed and documented. Unit contingency plans must document data backup.
(1.8.3) Workforce members are trained on the contingency access and data backup plans. Workforce must be trained on contingency plans

2. Technical Requirements

2.1 For systems containing confidential and/or regulated information and systems considered critical to the business, security architecture is documented, reviewed, and submitted to the UA ISO and relevant compliance offices. Approval of security architecture for regulated information must be granted by the compliance office prior to implementation.

ISO Policy only mandates that security architecture is approved for confidential and/or regulated information and systems considered critical to the business. However, the ISO recommends that security architecture be documented for all information and systems and that the documentation be protected in proportion to its security risk.

2.2 Methods are implemented to ensure the workforce and users agree with the terms of Acceptable Use of Computers and Networks Policy at least annually. Workforce and users who have an active UA NetID are automatically in compliance with this requirement.

2.3 All websites and applications that collect user information provide a visible link to the University Privacy Statement. The link to the University Privacy Statement should reference: https://www.arizona.edu/privacy

2.4 Identity and access management technical controls are implemented. Controls must include:
(2.4.1) Enforce the uniqueness of usernames. Access management utilizing a UA NetID are automatically in compliance with this requirement.
(2.4.2)Prevent re-assignment and transfer of usernames. Access management utilizing a UA NetID are automatically in compliance with this requirement.
(2.4.3)Require multi-factor authentication for users authorized to modify information. Access management utilizing the UA NetID+ system are automatically in compliance with this requirement.

2.5 Baseline vulnerability scans are performed and findings are addressed. Participation in the ISO Vulnerability Management program ensures compliance with these requirements. However, alternative solutions may be used. Vulnerability scanning must include:
(2.5.1) Network vulnerability
(2.5.2) Application vulnerability

2.6 Network devices are hardened. Hardening must meet the following requirements:
(2.6.1) Default passwords are changed using strong password methodologies.
(2.6.1) Device names are changed and default accounts are removed.
(2.6.1) Nonessential services are disabled and/or blocked.
(2.6.1) Access to management interfaces is restricted to nominated managed networks, management devices, or systems.
(2.6.1) Nonessential guest and world read access is disabled or blocked.

2.7 For Information Resources that house Confidential and/or Regulated information:
(2.7.1) Systems that house Confidential and/or Regulated data are segregated from systems that do not implement security controls sufficient to protect Confidential and Regulated data. The risk an information resource poses to other University systems must be considered.
(2.7.2) Only operating systems that are actively supported by the vendor and where the vendor is committed to providing ongoing security updates are connected to the network. Compensating controls may be used where appropriate.
(2.7.3) Remote access requires the use of a Virtual Private Network (VPN).
(2.7.4) Information is encrypted while in transit using cryptographic modules that meet industry best practices and are approved for use by UA ISO and any relevant compliance office. Adopt NIST approved algorithms.
(2.7.5) Systems generate access logs, which are aggregated and used to create activity reports. Network activity within the UA network is automatically monitored and used in the creation of activity reports. Application logs can be configured for aggregation and reporting through participation in the ISO Application Monitoring program.
(2.7.6) Data backup is implemented according to the backup plan.

3. Physical Requirements

3.1 Controls are implemented that limit physical access to systems containing Information Resources to authorized personnel only.

3.2 Controls that ensure visitor access is supervised at all times and logged are implemented.

3.3 Signage describing information security and privacy regulatory requirements for all relevant regulations are posted in work areas. Contact relevant UA compliance offices for details.

3.4 Signage describing information security and privacy reporting and response procedures are posted in work areas. Posting of the ISO Incident Response poster detailing security and privacy reporting and response procedures can be posted in work areas to satisfy this requirement.

Appendix – ISO Policy Compliance Requirements

Checklist key: ☑ = complete | ☐ = incomplete

☐ 1. Administrative Requirements

- ☐ 1.1 UA ISO Policies are well understood and easily accessible to the impacted workforce.
- ☐ 1.2 Workforce has received required information security, privacy, regulatory, and role based training.
- ☐ 1.3 Information security roles are assigned and communicated to the workforce and to UA ISO.
  - ☐ 1.3.1 Information Resource Owner(s) (Information Owners and Information System Owners)
  - ☐ 1.3.2 IT Security Manager(s)
  - ☐ 1.3.3 Information Security Risk Manager(s)
- ☐ 1.4 Unit procedures are aligned with UA ISO Policy and implemented and communicated to the workforce and to UA ISO.
  - ☐ 1.4.1 Unit information security and privacy procedures are defined and documented.
    - ☐ 1.4.1.1 Risk management and security planning procedures
    - ☐ 1.4.1.2 Information security and privacy audit response procedures
    - ☐ 1.4.1.3 IT Asset inventory procedures
    - ☐ 1.4.1.4 Information security and privacy event reporting procedures
    - ☐ 1.4.1.5 Access control determination and review procedures – physical and technical – user and administrator
    - ☐ 1.4.1.6 Supervision procedures for persons who work in areas where Confidential and/or Regulated data is accessible but who have not met the 'need to know' threshold
    - ☐ 1.4.1.7 Patch management procedures
    - ☐ 1.4.1.8 Vulnerability management procedures
    - ☐ 1.4.1.9 Physical access control procedures
    - ☐ 1.4.1.10 Workforce termination procedures
    - ☐ 1.4.1.11 Hardware and software license compliance assurance procedures
    - ☐ 1.4.1.12 Architecture and engineering procedures – architectural review, secure coding, etc.
    - ☐ 1.4.1.13 Device hardening procedures
    - ☐ 1.4.1.14 Activity report review procedures
  - ☐ 1.4.2 Workforce members are trained on and implement information security and privacy procedures.
- ☐ 1.5 Unit information security and privacy practices are established and enforced.
  - ☐ 1.5.1 Unit information security and privacy practices are determined and documented.
    - ☐ 1.5.1.1 Role based information security and privacy training requirements
    - ☐ 1.5.1.2 Periodicity and method(s) of compliance evaluation
    - ☐ 1.5.1.3 Vendor and contract review and management
    - ☐ 1.5.1.4 Use of removable media
    - ☐ 1.5.1.5 End user device protection and BYOD
    - ☐ 1.5.1.6 Information retention and disposal
  - ☐ 1.5.2 Workforce members incorporate information security and privacy practices into their business processes.
  - ☐ 1.5.3 MOUs, SLAs, EULAs, and other agreements entered into with customers describe relevant information security and privacy practices.
  - ☐ 1.5.4 Vendor agreements are reviewed to confirm compliance with UA ISO Policy and unit/program practices.
- ☐ 1.6 Third party and regulatory information security and privacy requirements are met.
  - ☐ 1.6.1 Information resources are assessed, in collaboration with UA ISO and compliance offices, to determine regulatory implications.
  - ☐ 1.6.2 Information security and privacy practices are reviewed and approved by appropriate compliance offices.
  - ☐ 1.6.3 Information security and privacy practices are assessed against contracts and agreements, such

as DTAs/DUAs, that impose requirements on the unit/program.

☐ 1.7 Information resources are identified and managed.

☐ 1.7.1 IT Assets are inventoried and characterized according to system criticality and information classification.

☐ 1.7.2 Information, data, collections, etc. are identified, inventoried, and classified according to UA Data Classification Standard.

☐ 1.8 For systems containing confidential and/or regulated information and systems considered critical to the business, contingency access and data protection planning has been performed.

☐ 1.8.1 A contingency access plan has been developed and documented.

☐ 1.8.2 A data backup plan has been developed and documented.

☐ 1.8.3 Workforce members are trained on the contingency access and data backup plans.

☐ 2. Technical Requirements

☐ 2.1 For systems containing confidential and/or regulated information and systems considered critical to the business, security architecture is documented, reviewed, and approved by UA ISO and relevant compliance offices

☐ 2.2 Methods are implemented to ensure the workforce and users agree with the terms of Acceptable Use of Computers and Networks Policy at least annually.

☐ 2.3 All websites and applications that collect user information provide a visible link to the University Privacy Statement.

☐ 2.4 Identity and access management technical controls are implemented.

☐ 2.4.1 Enforce the uniqueness of usernames.

☐ 2.4.2 Prevent re-assignment and transfer of usernames.

☐ 2.4.3 Require multi-factor authentication for users authorized to modify information.

☐ 2.5 Baseline vulnerability scans are performed and findings are addressed.

☐ 2.5.1 Network vulnerability

☐ 2.5.2 Application vulnerability

☐ 2.6 Network devices are hardened.

☐ 2.6.1 Default passwords are changed using strong password methodologies.

☐ 2.6.2 Device names are changed and default accounts are removed.

☐ 2.6.3 Nonessential services are disabled and/or blocked.

☐ 2.6.4 Access to management interfaces is restricted to nominated managed networks, management devices, or systems.

☐ 2.6.5 Non-essential guest and world read access is disabled or blocked.

☐ 2.7 For Information Resources that house Confidential and/or Regulated information:

☐ 2.7.1 Systems that house Confidential and/or Regulated data are segregated from systems that do not implement security controls sufficient to protect Confidential and Regulated data.

☐ 2.7.2 Only operating systems that are actively supported by the vendor and where the vendor is committed to providing ongoing security updates are connected to the network.

☐ 2.7.3 Remote access requires the use of a Virtual Private Network (VPN).

☐ 2.7.4 Information is encrypted while in transit using cryptographic modules that meet industry best practices and are approved for use by UA ISO and any relevant compliance office.

☐ 2.7.5 Systems generate access logs which are aggregated and used to create activity reports.

☐ 2.7.6 Data backup is implemented according to the backup plan.

☐ 3. Physical Requirements

☐ 3.1 Controls are implemented that limit physical access to systems containing Information Resources to authorized personnel only.

☐ 3.2 Controls that ensure visitor access is supervised at all times and logged are implemented.

☐ 3.3 Signage describing information security and privacy regulatory requirements for all relevant regulations are posted in work areas.

☐ 3.4 Signage describing information security and privacy reporting and response procedures are posted in work areas.