Supplemental Guidance on Guidelines for Data Protection

This information is intended to give guidance for meeting the Guidelines for Data Protection, including examples, specific periodicity and specific methods. This guidance is not going to be appropriate for all environments, but they provide a starting point for individuals asking questions such as "how often is periodically". This guidance incorporates common regulations, and may be too restrictive for many.

AC-6 Access to Institutional Data is reviewed and reauthorized by a Data Steward or a delegate on a periodic basis

For this purpose, periodic is at least once every year. Some regulations may require reauthorization more frequently.

AC-8 Active sessions require re-authentication after a period of inactivity

For this purpose, a period of inactivity is 15 minutes. This is 15 minutes of no activity. If there is activity, there is no need to re-authenticate.

AC-13 Screen locking that hides the working screen after a period of inactivity (e.g. screensavers) is required

Similar to AC-8, the period of inactivity is 15 minutes. Many cloud tools don't support any type of screen locking themselves. Locking the workstation accessing that application/tool meets the intent of this control.

AL-4 Logs are reviewed on a periodic basis for security events

The period depends significantly on the volume of logs that are being reviewed. For a system housing restricted data, at least daily is recommended, for a system housing private data, at least weekly is recommended.

ISO also recommends using a tool to automatically parse the logs for known events, alerting administrators or users to those events. These tools are reviewing the logs constantly on behalf of the administrator.

DR-1/DR-2 A disaster recovery/business continuity strategy is implemented and tested periodically

The importance of the system will dictate the periodicity of testing the DR/BC strategy, however, ISO recommends at least annually.

DR-3 Backup copies are protected at least as well as primary data

If backup copies of data are created, these copies should be protected at least as well as the primary data. If the backup is a hot spare, that system or set of systems should be almost identical to the primary system. If the backup is a set of tapes, those tapes should be physically protected as well as the primary systems, and if they are "online", the Information Systems that control access to the data should be as close to the control implementation as the primary system as possible. Removeable media (such as tape) that contains private or restricted data must be encrypted per EN-3

EN-6 Approved Algorithms and key-lengths are used where encryption or digital signing are employed

Approved algorithms will change over time as cryptography research advances and computational power increases. All FIPS tested algorithms and key-lengths are considered approved. Other approved algorithms and key lengths will continue to be published at https://www.cmu.edu/iso/governance/guidelines/data-protection/encryption-guidance.html

Data use agreements may specify stronger algorithm requirements, and those should be followed where applicable. Where a data use agreement allows for weaker cryptography than the University's standards, the University's standards will prevail.

EN-7 Keys are changed periodically where encryption is employed

Periodic changes to encryption keys should be balanced against the risk to the data or systems that the key protects and the difficulty of changing those keys. Keys should always be changed immediately if they are suspected compromised (for example, SSH keys) or the individual with control of them has left the University or changed positions (EN-9). Otherwise, every 5 years with an annual analysis of the risk to the data is recommended.

ID-5 Inactive Identifiers are disabled after a defined period of time

Inactive identifiers are those that have not had a successful login for a period of time. The recommended time period is 30 days, however, the use of two-factor authentication can mitigate the concerns around un-used accounts and allow for longer periods of inactivity. The inconvenience to users can be mitigated by the use of a self-service identity verification solution: such as security questions, or alternative email addresses.

ME-1 Electronic Media is sanitized prior to reuse and ME-2 Electronic and paper-based media is destroyed prior to disposal

Media sanitization and disposal methods vary based on the media and/or device housing that media. NIST SP800-88 Appendix A (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
) provides guidance on acceptable methods.

Contracting with a 3rd party to perform this sanitization or destruction is acceptable, as long as they follow the minimum requirements and provide assurance (such as a certificate of destruction) that the sanitization or destruction occurred.

ME-4 Mark removeable media with the data classification where it may be accessed outside of an authorized group of individuals

At a minimum, the University's restricted data should be marked in some way to indicate its classification level. This could be a label on the media or container, it could be a header or footer on a document, etc. The goal is that anyone who comes across the media that wouldn't already know it's classification by virtue of their job position is aware of how to protect it. For example, I-9 forms within a Human Resources office area. They would only need marking if they left that area, as all individuals working with I-9 forms are aware of the classification of those forms by virtue of their job position.

If the Data is entrusted to the University by a third-party, that third-party may have specific marking requirements that should be followed.

NS-6 Network access controls are reviewed on a periodic basis for appropriateness

Network access controls should be reviewed at least annually, some regulations require every 6 months or every 90 days.

PE-1 All individuals are screened prior to accessing Institutional Systems

The appropriate screening will depend on the system(s) and data being accessed for the individual's role at the University. Human Resources provides for background checks through their Staff Background Check Policy:

https://www.cmu.edu/hr/assets/hr/restrict/staff-background-check-policy.pdf . Other processes exist for screening individuals prior to granting access to Institutional Systems, such as the collaborative visitor process, and export controls https://www.cmu.edu/research-compliance/export-controls/index.html.

CM-4 Controls deployed to protect against malicious code scan the entire system periodically

The periodicity of this scan will depend on the particular system and it's use and load, but ISO recommends at least once every 30 days.

CM-13 Operating system and software security patches are deployed in a timely manner

ISO's recommendation is at least within 30 days of release by the vendor. There may be times when a particular patch may need to be deployed more quickly, such as when an active exploit is being seen on the network. There may also be times when a patch should be delayed due to adverse impacts. Patches that are delayed past 30 days after release should have compensating controls in place to protect the data on that system.

CM-21 Review all configuration changes for security impacts

Reviewing configuration changes for security impacts ensures that a vulnerability is not unintentionally introduced as part of a change. Some changes may be "pre-approved", such as applying a vendor security patch. Some may involve further review such as adding a new service to the system.

AS-2 System is periodically tested for security vulnerabilities (e.g. vulnerability scanning, penetration testing, etc.)

Automated vulnerability scans should be conducted at least monthly, more often if the Information System is a publicly accessible system (such as a web server). At a minimum, vulnerability scanning should be conducted after a major change to the system that affects what ports, services, or applications are exposed. Some systems may react adversely to automated scanning, and the schedule for those systems should take into account the purpose of the system, the data stored on the system, and the affects automated scanning has on the system. ISO offers automated vulnerability scanning to campus Information Systems. Penetration testing is more in-depth testing of an information system, and should occur as often as necessary for the purpose of that system. A recommendation is every 3-5 years, or if a major change occurs in the architecture of the environment.

AS-3 Periodically audit systems for adherence to controls

Systems should be reviewed at least every two years to ensure that the controls that are expected to be in place remain in place. Some regulations require an annual audit. Automated audits (such as those that configuration management systems perform, i.e. SCCM, Puppet, etc) may be conducted for controls that lend themselves to it.