Collin College Technology Services (CC-TS)
Computer Compliance – Risk Assessment ISP

PURPOSE

The purpose of this ISP is for Collin College Technology Services to assess risks to information assets and manage those risks effectively by reducing threats of impairment to the confidentiality, integrity, and availability of such assets. A standard risk assessment methodology and management process will be used for all systems to create, store, process, or transmit internal, confidential, restricted, or critical information.

ISP STATEMENT

Collin College (CC) Chief Information Security Office (CISO)will conduct risk assessments on all information technology systems, devices, and related equipment, excluding isolated devices designated for instruction, and update such risk assessments to manage risks effectively. Information systems/application risk assessments must be conducted annually and as part of the procurement process for all systems.

RISK ASSESSMENT

1. The risk assessment process identifies and assesses risks associated with information assets and defines cost-effective solutions to managing those risks.

2. An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of information should be conducted for all systems and applications that contain confidential or restricted information. The scope of the risk assessment will include the administrative, physical, and technical controls as required by law and CC privacy and security policies.

3. Risk assessment is the first and one of the most critical steps in the security management process. Assess risks to those assets and develop countermeasures to those risks must be conducted. In addition, implementations of other CC security policies and ISPs depend on the thoroughness and quality of risk assessment.

FREQUENCY OF SYSTEM AND PHYSICAL SECURITY ASSESSMENTS

At a minimum, risk assessments on all assets attached to the college network will be conducted and reviewed annually. Risk assessments will be completed more frequently as indicated on the assets identified below:

1. Monthly: High impact – High data-value
    a. PCI-DSS Compliant assets
    b. CJIS assets
    c. HIPAA Related servers and nodes
    d. Primary Microsoft AD Controllers
    e. BANNER Servers
    f. Servers and Services with assigned public IP address

2. Quarterly: High impact – Low data-value
    a. Core data switches
    b. Distribution layer switches
    c. WiFi Controllers
    d. Internal support server, e.g., DNS, WSUS, SCCM, TRANE, etc.
    e. Cisco VoIP servers, Cisco FTD/FMC
    f. Netmotion, RSA, CBORD, etc.

3. Annually: Low impact – Low data-value
    a. Workstations
    b. Cisco VoIP phones
    c. Cisco Access Points
    d. ASSA Abloy locks
    e. CBORD Control Panels
    f. Industrial Internet of Things – e.g., Lighting controllers, HVAC controllers, etc.

In addition, assessments shall be performed under each of the following special circumstances:

- Purchase, acquisition, or system procurement
- Part of the system development/modification/upgrade process and maintenance
- When changes are to be made to the infrastructure (e.g., remodeling, additions, installation, etc.)
- Upon notification of a vulnerability or violation or breach of privacy or security
- The system owner/unit manager is responsible for implementing changes in policies, procedures, and system modifications necessary to mitigate security risks to an acceptable level based on assessment findings.

STANDARD RISK ASSESSMENT PROCESS

The standard risk assessment process to be used should include the following:

1. Assignment of responsibilities for risk assessment, including appropriate participation of executive, technical, and other management staff as necessary.

2. Identify the information assets at risk, particularly information technology applications critical to business operations.

3. Identify the threats to which the information assets could be exposed.

4. Assessment of the vulnerabilities, i.e., the points where information assets lack sufficient protection from identified threats. Vulnerability scans will be completed on all assets using the following criteria:

    a. Authenticated Qualys Scans on the following nodes:
        i. Microsoft Primary AD controllers
        ii. Bursar Computers – PCI DSS
        iii. All Microsoft college servers and services with Public/Internet IP addresses

    b. Unauthenticated Qualys Scans on all other nodes and devices

5. Determination of the impact of loss, based upon quantitative or qualitative assessment of a realized threat for each vulnerability and an estimation of the likelihood of such occurrence. Note: As part of the determination, actual or planned countermeasures, which may be installed, must be ignored and considered not present. This is because it is the intrinsic importance (value) of the data itself which needs to be assessed. If existing countermeasures were considered, this would artificially deflate the essential value of the data. The fact that the security breaches may be countered or the consequences prevented or minimized is irrelevant to the assessment.

6. Identify and estimate the cost of protective measures that would eliminate or reduce the vulnerabilities to an acceptable level of risk.

7. Selection of cost-effective security management measures to be implemented.

8. Preparing a final report to be submitted to the Data Owner and kept on file by the department, documenting the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of remaining risk to be accepted.

RISK ASSESSMENT STEPS

The computer security risk management guidance published by the National Institute for Standards and Technology (NIST) in its Special Publication (SP) 800-30 Rev. 1 titled "Guide for Conducting Risk Assessment" should be used as a guide in conducting information security risk assessments compliant with the above requirements. This publication describes risk assessment steps that should be used in performing the required risk assessments. Scoring has been added to each required area as necessary.

Step	Action	Description
1.	System Characterization	Document the system/application, purpose, owner or responsible person(s), department, location, contact information, function, connectivity, number and type of users, physical environment description, and system/application criticality.
2.	Threat Identification	Identify the potential threat sources and compile a list of potential threat sources and associated vulnerabilities that apply to the evaluated system. This list is compiled and applied through the Qualys-hosted system. Each listed threat is then assigned a score based on its threat to one or more of the required confidentialities, integrity, and availability requirements. Threat identification is managed and assigned by Qualys and updated weekly.
3.	Vulnerability Identification	Identify flaws or weaknesses that could be exercised to result in a security breach or violation of the system's security policy. Each of the listed threats/vulnerabilities is assigned a score by Qualys based on the threat it poses to one or more of the required confidentiality, integrity, and availability requirements.
4.	Impact Analysis	Determine the adverse impact of a successful threat exercise of vulnerability. The negative impact shall be categorized accordingly: loss of integrity, availability, and confidentiality. Impact Analysis for any breach of discovered vulnerability must always include damage to reputation, resulting in financial loss.

5.	Likelihood	To derive an overall rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment. Determine the likelihood that this threat will occur if no safeguards are in place to prevent it. There is a high probability of internal vulnerability scans if no safeguards exist.
6.	Control Analysis	Analyze the controls that have been implemented, or are planned for implementation, to minimize or eliminate the likelihood (or probability) of a threat exercising a system vulnerability. Note: If safeguards are in place, such safeguards serve as a countermeasure to the associated threat, thereby reducing the risk that a threat/vulnerability will occur to an acceptable level.
7.	Risk Score Determination	Calculate the level of risk to the system/application to determine its overall risk. Threat Vulnerability could result in Loss of Confidentiality, Integrity, and Availability (CIA). Calculated threat levels are determined by Qualys and assigned as listed below: 1. Severity 5 – Urgent 2. Severity 4 – Critical 3. Severity 3 – Serious 4. Severity 2 – Medium 5. Severity 1 – Minimal
8.	Remediation/ Mitigation	Controls/Safeguards to mitigate (reduce) or eliminate the identified risks, as appropriate, must be identified, and corrective action must be taken for systems/applications with known vulnerabilities discovered during the Qualys scan. Mitigation is recommended within the timelines listed below: 1. Severity 5 – 48 Hours 2. Severity 4 – 7 Days 3. Severity 3 – 14 Days 4. Severity 1 & 2 – 30 Days Strict adherence to these timelines is required for devices that must meet PCI, HIPPA, FERPA, and CJIS requirements or has a publicly accessible IP address.
9.	Results Documentation	Once the risk assessment and mitigation have been completed, the results will be documented and provided to the designated data owner.

RISK MANAGEMENT

System owners and department managers/supervisors are responsible for risk management. These decisions must be based on the results of the required risk assessment process above. The department manager/application owner is responsible for prioritizing, implementing, and maintaining the appropriate risk-reducing measures identified from the risk assessment process.

Implementation of security measures sufficient to reduce risks and vulnerabilities to information systems and resources to a reasonable and appropriate level is required to:

- Ensure the confidentiality, integrity, and availability of all sensitive information created, received, maintained, or transmitted.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required
- Ensure compliance with this policy by department staff, contract providers, vendors, and business associates

If the risk is sufficiently severe, or if no remediation occurs within the timeline identified above, Information Security staff may, with the approval of the CISO, remove the asset from operation by blocking it at the internal or external firewall or by any other means sufficient to prevent the machine from being compromised. The system owner shall be notified before removing the system from service or as soon as it is feasible thereafter.

RESIDUAL RISK

Even after implementing all security controls, no covered entity will be 100 percent risk-free or 100 percent secure. Many times, after security controls are implemented, there is some amount of risk remaining, which is called residual risk. In addition, a residual risk exists when a decision is made to accept a risk due to the cost of the control being high or the likelihood or impact of the threat being low. Management must determine the amount of residual risk to accept. The risk assessments should provide leadership with enough information to make decisions about residual risks.

There are four basic ways of addressing residual risk:

1. Transferring - If management decides that the total or residual risk is too high, it may purchase insurance to offset any costs should the risk be realized. They are transferring the risk to the insurance company for a cost less than the control.

2. Rejecting - If management ignores the risk, they reject it in theory but practically accept it because the risk and the liability do not just disappear (see number 4 below - Accepting risk).

3. Reducing - If management implements controls, they reduce or mitigate the risk.

4. Accepting - If management decides to live with the identified risk, they accept its impact should it be realized. Usually, the "residual" risk is accepted AFTER mitigating or correcting the initial risk and lowering it to an acceptable level.

INFORMATION SYSTEMS ACTIVITY REVIEW (Periodic Review of Internal Security Controls)

Each information system owner/responsible unit must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports to identify discrepancies between policies and practices. A "system" typically includes hardware, software, information, data, applications, communications, and people.

- Monitoring should be performed by use of the audit capabilities of the access control software system and through the internal creation and use of programs specific to this purpose as approved by the Designated Information Recourse Manager (IRM) and CISO.
- Upon notification of any abnormal activity, the information system/application owner/responsible department must review the incident and take appropriate action and follow-up.

PERIODIC PHYSICAL SECURITY RISK ASSESSMENT

Each department area will:

- Establish and document procedures for performing periodic self-assessments of security controls.
- Perform initial and periodic risk assessments on systems processing or storing confidential or restricted information.
- Maintain risk assessments in secured files. Mitigate identified problems.
- Forward risk assessments to the CC IRM, CISO, or Internal Auditor office upon request

Related Policies, References, and Attachments:

An index of approved CC-TS ISPs can be found on the CC Technology Services ISP's website at https://www.collin.edu/security. Reference materials, legal compliance guidelines, and ISP enforcement are available in the IA-ISP Compliance Document. The CC Information Security Program and CC Information Security User Guide are available on the Information Technology Services Policies website.

Implementation Information

Review Frequency:	Annually
Responsible Person:	CIO/IRM
Approved By:	SVP, Campus Operations
Approval Date:	12/13/2022

Revision History

Version:	Date:	Description:
1.0	12/12/2022	Initial document
1.1	3/21/2024	Annual Review – No changes.