Exception Procedure

Scope

This exception procedure applies to the entire organization; University of Rochester, including the Medical Center, all Affiliates, and the organization workforce.

The organization published governing Information Security Policies and Standards are applicable to the entire organization. Refer to Tech. Rochester. https://tech.rochester.edu/information-security-policies-procedures-old/full-information-security-policies-procedures-2/.

Exception Requirements

For all planned and identified non-compliance with organization published information security policies and standards, this exception procedure is required, with justified, documented, senior management-approved information security policy exceptions and implemented alternative security controls.

Some examples of information security policy non-compliance scenarios where exceptions may be required include:

- Medical devices that are unable to encrypt stored high risk PHI data,
- Systems, applications, and / or devices that are running on outdated and unsupported operating systems,
- Conducting business functions on personally owned computing devices not under an organization managed mobile device management program,
- Not leveraging multi-factor authentication for remote access or other specified access,
- Not leveraging email banners or scanning for external incoming emails,
- Not updating vendor applications with latest security upgrades and patches,
- Not implementing required timeframes for screen lockout or session disablement,
- Not complying with applicable security-related regulations or other organization business security obligations, and,
- Not leveraging security best practices.

Exception Request Forms, Content, and Submission

Exception requesters can use the Exception Request Online Form https://tech.rochester.edu/forms/deferral-request/ or the Risk Acceptance Form available from the Information Security Risk and Compliance team at InfoSecRiskandComp@URMC.Rochester.edu.

All fields must be completed to the best of the requester's knowledge. Exception requests should include at least the following information if known:

- Submission date, requester name, contact information, and department,
- Appropriate business manager approval,
- Impacted information security procedure or function,
- Description of the non-compliance scenario,
- Business justification for the non-compliance scenario,

- Assessment of risks or threats resulting from non-compliance,
- Proposed plan for managing risk associated with non-compliance (e.g., alternate risk mitigating controls in place or that could be put in place),
- Proposed plan and dates for resolving the non-compliance,
- Estimated dates for duration of the exception,
- Impacted devices if applicable (manufacturer, model, operating system, other information),
- Additional helpful comments and information if pertinent.

Exception requesters must ensure the appropriate supervisor, manager, or director has seen the request, agrees, and approves with their name and contact information entered on the form.

Submitted Exception Request Online Forms are automatically emailed to the Information Security Risk and Compliance team. (Click on the "Submit" icon at the bottom of the form). If using the Risk Acceptance Form, exception requesters should email completed forms to the Information Security Risk and Compliance team at InfoSecRiskandComp@URMC.Rochester.edu.

Information Security Risk and Compliance Review

The Information Security Risk and Compliance team reviews exception request submissions and works with exception requesters and other applicable individuals to complete any missing information.

Exception scenarios, mitigating controls, resolution plans, and other key information are reviewed. Issues with provided information are addressed. Residual risks and risk levels are determined by the information Security Risk and Compliance team.

The Information Security Risk and Compliance team enters all exceptions (draft, pending, approved, denied, etc.) in the organization Governance, Risk, and Compliance (GRC) exception repository tool, and manages exceptions to resolution and closure.

URMC and Affiliates Exception Requests

The Information Security Risk and Compliance team provides exceptions related to URMC and Affiliates to the URMC and Affiliates Exception Committee for detailed review, approval, or denial.

The URMC and Affiliates Exception Committee is responsible to acknowledge, understand, and approve or deny all new and extension URMC and Affiliates exception requests. For approved requests, the committee understands they are accepting the exception residual risks and risk level for the organization.

University Exception Requests

Exception requests related to the University are not provided to the URMC and Affiliates Exception Committee and are instead considered already approved from the appropriate supervisor, manager, or director approvals on the forms. Those managers must understand they are accepting the exception residual risks and risk level for the organization.

Information Security Risk and Compliance Exception Record Management

The Information Security Risk and Compliance team sets the initial expiration date at maximum one year, with required reviews and status updates re-obtained at expiration date. If non-compliance scenarios have been verified as resolved, the exceptions can be closed. If non-compliance scenarios are still required, justified extensions of maximum one-year intervals can be requested, and must be approved, with additional reviews and status updates at subsequent expiration dates.

Contact the Information Security Risk and Compliance team at InfoSecRiskandComp@URMC.Rochester.edu with any questions.