Weill Cornell Medicine

11.20

Variances

Responsible Executive: Chief Information Officer, Weill Cornell Medicine
Original Issued: September 12, 2023
Last Updated: September 12, 2023
Last Reviewed: September 12, 2023

Contents

Policy Statement

All members of the Weill Cornell Medicine community are responsible for protecting the confidentiality, integrity, and availability of information created, received, stored, transmitted, or otherwise used by the college, and for college activities performed by authorized parties (hereinafter referred to as “data”). All devices used for Weill Cornell Medicine purposes, regardless of ownership, must meet the minimum security and system requirements defined in ITS policies. In the event that a policy cannot be met, a variance request must be submitted to ITS along with appropriate justification and compensating controls.

Reason for Policy

Weill Cornell Medicine requires a minimum set of security requirements for devices accessing Weill Cornell Medicine networks, applications, and data or used for Weill Cornell Medicine purposes. By mandating a minimum set of security requirements, Weill Cornell Medicine can reduce the risk of an adverse event. In the event that a security requirement cannot be met, Weill Cornell Medicine must still ensure that data is protected. Variances will be evaluated in extenuating circumstances and may be approved with adequate justification and risk mitigating compensating controls.

Entities Affected by this Policy

All units of Weill Cornell Medicine, including Weill Cornell Medicine-Qatar.

Who Should Read this Policy

All members of the Weill Cornell Medicine community utilizing Weill Cornell Medicine information technology resources, including devices not owned by Weill Cornell Medicine but used for Weill Cornell Medicine purposes.

All stewards and custodians of Weill Cornell Medicine data.

Web Address of this Policy

https://its.weill.cornell.edu/policies

Contacts

Direct any questions about this policy, 11.20 – Variances, to Brian J. Tschinkel, Chief Information Security Officer, using one of the methods below:

- Office: (646) 962-2768
- Email: brt2008@med.cornell.edu

1. Principles

Variances to ITS policies increase the risk of an adverse event or loss of Weill Cornell Medicine data's confidentiality, integrity, or availability. Requests for approval of variance shall be considered in relatively unusual circumstances only when certain criteria are met. Variances are temporary and must be renewed at least annually, must have adequate justification, and must have demonstrated compensating controls to reduce the risk of an adverse event to an acceptable level. Variance requests must be submitted to ITS with approval from the individual's department administrator.

2. Variance Types

2.01 Encryption

Pursuant to ITS policy 11.06 – Device Encryption, all members of the Weill Cornell Medicine community must take care to protect high risk data (as defined in ITS policy 11.03 – Data Classification) on their devices, including laptops, desktops, smartphones, and tablets. All devices owned by Weill Cornell Medicine must be encrypted, and devices not owned by Weill Cornell Medicine but used for Weill Cornell Medicine purposes must adhere to the appropriate safeguards defined in the Device Encryption policy.

Variances to device encryption shall be considered only when the following conditions are met:

1. The device is demonstrated not to contain high risk data,
2. The individual attests that the device will never be used for high risk data,
3. The device does not meet the minimum hardware requirements to support encryption and cannot be upgraded or encryption is known to be incompatible with a Weill Cornell Medicine application,
4. No practical encrypted alternative is available such as centralized file storage services or self-encrypting hard drives, and
5. The device is demonstrated to be physically secured from loss or theft.

There is significant risk in not encrypting devices used to access Weill Cornell Medicine high risk data, and a breach may result in regulatory sanctions and fines for the College and the individual responsible for the data.

2.02 Operating System Upgrades or Updates

Pursuant to ITS policies 11.10 – Device Minimum Security Requirements and 11.11 – Requirements for Securing Systems, devices used for Weill Cornell Medicine purposes must use a modern operating system that regularly receives security updates from the manufacturer.

ITS management software ensures operating systems are kept up to date by regularly deploying upgrades and updates. Variances to operating system upgrades or updates shall be considered only when either of the following conditions are met:

1. The operating system upgrade or update is known to be incompatible with a Weill Cornell Medicine application, or
2. A third-party vendor is managing and deploying operating system upgrades or updates at the same cadence as ITS on managed devices (see ITS policy 11.12 – Restricting Access for Insecure Systems).

Devices which are able to receive operating system upgrades and updates from ITS but require a different deployment schedule do not require a variance. A request for a different deployment schedule may be submitted to ITS.

2.03 Application Upgrades or Updates

Pursuant to ITS policies 11.10 – Device Minimum Security Requirements and 11.11 – Requirements for Securing Systems, devices used for Weill Cornell Medicine purposes must be configured to regularly or automatically install security updates from application developers.

ITS management software ensures applications are kept up to date by regularly deploying upgrades and updates. Variances to application upgrades or updates shall be considered only when either of the following conditions are met:

1. The application upgrade or update is known to be incompatible with a Weill Cornell Medicine application, or
2. A third-party vendor is managing and deploying application upgrades or updates at the same cadence as ITS on managed devices (see ITS policy 11.12 – Restricting Access for Insecure Systems).

2.04 Endpoint Detection and Response/Anti-virus/Anti-malware

Pursuant to ITS policies 11.10 – Device Minimum Security Requirements and 11.11 – Requirements for Securing Systems, devices used for Weill Cornell Medicine purposes must have an endpoint detection and response (EDR), anti-virus (AV), or anti-malware (AM) product that is installed, enabled, and regularly updated.

ITS management software ensures an EDR/AV/AM product is installed, enabled, and regularly updated. Variances to installing the ITS EDR/AV/AM product are considered only on exceptional circumstances and only when the following conditions are met:

1. The EDR/AV/AM product is proven to be incompatible with a Weill Cornell Medicine application, cannot be configured with exclusions to monitoring specific files or folders, and cannot be tuned to minimize the impact to running a Weill Cornell Medicine application; or
2. A third-party vendor is installing, enabling, and regularly updating a comparable EDR, AV, or AM product.

2.05 System Management

Pursuant to ITS policy 11.10 – Device Minimum Security Requirements, devices owned or issued by Weill Cornell Medicine must have ITS management software installed. ITS management software ensures devices are inventoried, receiving regular security updates, compliant with applicable policies, and traceable and wipeable in the event of loss or theft.

Variances to system management shall be considered only when the system management software is known to be incompatible with a Weill Cornell Medicine application. As the system management software also enables device encryption, installs EDR or AV software, and deploys operating system and application updates and upgrades, additional variances may also be required as described in the previous sections.

Revision History:

Date	Author	Revision
September 12, 2023	Brian J. Tschinkel	Initial release