RUSH	**Policy Title:** Acceptable Use of Information Technology Resources Policy	**Policy Number:** N/A

Document Owner: Kristin Parker		**Approver(s):** Michael Levinson	
Date Created: 10/20/2025	**Date Approved:** 10/20/2025	**Date Updated:** 11/24/2025	**Review Due:** 10/20/2026
Applies To: RUMC ☒ RMG ☒ ROPH ☒ RCMC ☒ RU ☒			

Printed copies are for reference only. Please refer to the electronic copy for the latest version

Contents

Contents 1
1. Purpose 2
2. Scope 2
3. Policy 2
   3.1 General Use Topics 2
   3.2 User Accounts and Access 4
   3.3 Data Protection 5
   3.4 Email and Communication 6
   3.5 Software and Applications 6
   3.6 Rush Owned or Managed IT Devices and Assets 7
   3.7 BYOD/ Personal Devices 8
4. Monitoring 9
5. Applicability 9
6. Associated Documents 9
7. Disclaimer 10
8. Revision History 11
9. Approval History 11

Policy Title: Acceptable Use of Information Technology Resources Policy		**Policy Number:** N/A	
Document Owner: Kristin Parker		**Approver(s):** Michael Levinson	
Date Created: 10/20/2025	**Date Approved:** 10/20/2025	**Date Updated:** 11/24/2025	**Review Due:** 10/20/2026
Applies To: RUMC ☒ RMG ☒ ROPH ☒ RCMC ☒ RU ☒			

1. Purpose

This Acceptable Use of Information Technology Resources Policy ("Policy") outlines the appropriate use of Information Technology ("IT") resources at Rush University System for Health ("Rush" or "system").

These technology resources include computer systems, third-party data storage and transfer applications, networks, internet access, email, software, hardware, data, and telecommunications equipment. This policy applies to all these resources regardless of ownership or location, when used for Rush business or accessed via Rush's networks.

This policy's goal is to ensure the security, confidentiality, integrity, availability, and ethical use of these resources in support of Rush's iCARE values – innovation, collaboration, accountability, respect, and excellence. (For more details: Mission, Vision, and Values | Rush.)

2. Scope

This policy applies to all individuals who use Rush IT resources, including employees, staff, faculty, students, medical fellows and residents, volunteers, visiting scholars, contractors, affiliated personnel, and any other individuals granted access to Rush IT resources. Rush patients and visitors may access the Rush Visitors network and are not covered by this policy.

3. Policy

Anyone using Rush IT resources must comply with our system's policies, standards, procedures, guidelines, and any applicable license agreements and laws, including federal, state, local, and intellectual property laws. Below, we outline the requirements and expectations for the acceptable use of Rush IT resources.

3.1 General Use Topics

All Rush IT resources are Rush's property or are appropriately licensed by their owners and are provided for the primary purpose of conducting Rush business.

Policy Title: Acceptable Use of Information Technology Resources Policy		**Policy Number:** N/A	
Document Owner: Kristin Parker		**Approver(s):** Michael Levinson	
Date Created: 10/20/2025	**Date Approved:** 10/20/2025	**Date Updated:** 11/24/2025	**Review Due:** 10/20/2026
Applies To: RUMC ☒ RMG ☒ ROPH ☒ RCMC ☒ RU ☒			

Rush IT users must protect classified information when using these systems. This information includes corporate, patient, student, employee, personal, private, or restricted information, such as Personally Identifiable Information (PII) and Electronic Patient Health Information (ePHI).

As a Rush IT user, you may use IT resources for occasional personal needs, provided these uses are necessary and infrequent. You should never conduct personal business on a Rush IT resource in an area where the device screen is visible to others. It is up to you to ensure that your personal use of Rush IT systems complies with other Rush policies, does not burden Rush systems, and does not impede anyone's ability to perform their duties and responsibilities in fulfilling Rush's mission. Failure to comply with Rush policies may result in the loss of this privilege.

As you review these dos and don'ts, keep in mind that our Rush values require that we be accountable for our actions, respectful of others (and their private data), and willing to learn. Protecting private information (whether it belongs to staff, students, patients, or other members of our community) is one of the important expressions of those values, and is required for all participants on Rush's networks and systems.

Do (Acceptable Use)

1. Follow all information security guidelines established by Rush D&IS.
2. Report any suspicious activities or potential security breaches immediately to the IT Service Desk.

Don't (Unacceptable Use)

1. Engage in any activity that violates local, state, or federal laws or regulations.
2. Bypass or circumvent Rush's information security controls.
3. Tamper with or disable security measures on Rush IT assets (e.g., bypassing user authentication requirements, disabling antivirus software).
4. Access websites that could pose a security risk or contain content inappropriate for the workplace. (If you're not sure, don't visit the site.)
5. Connect non-approved IT resources (e.g., software, hardware, Internet of Things (IoT) devices, AI tools, etc.) to any Rush IT resource, including the Rush wireless network.

6. Use shared or medical computers, or computing devices, e.g., smartphones, tablets, or public kiosks, to log into non-Rush work systems or applications, to conduct personal business, to create anonymous online posts, or in any way violate this policy.
7. Violate content owners' copyright. You are allowed to use brief excerpts from copyrighted works under Fair Use standards. If you are unsure whether a given use of copyrighted work is allowed, contact the Rush Legal Team for guidance.
8. Distribute, transmit, post, or store any electronic communication that is threatening, obscene, harassing, pornographic, hearsay-driven, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate.
9. Propagate chain letters, fraudulent mass mailings, disinformation, spam, or other undesirable and unwanted email content using Rush IT resources.
10. Use Rush IT resources to circulate unauthorized solicitations or advertisements for non-system purposes, including religious or political initiatives, or community activities (Girl Scout Cookie Drives, etc.).
11. Use Rush information or IT resources for commercial or personal purposes, in support of for-profit activities, outside employment, or business activity (e.g., consulting for pay, business transactions, making fraudulent offers of products, items, or services, etc.).

3.2 User Accounts and Access

Do (Acceptable Use)

1. Only use your assigned Rush computer accounts when conducting Rush business. Users are responsible for all activities associated with their accounts.
2. Create strong, unique passwords and change passwords regularly as required.
3. Only approve Multi-Factor Authentication ("MFA") prompts for logins you initiate. Always review requests carefully to prevent security incidents.
4. Log off from any Rush device whenever you're going to stop using it actively. This is especially important if the device has multiple users.
5. Report suspicious and unauthorized user account logins to the D&IS Service Desk.

Don't (Unacceptable Use)

1. Share or reveal passwords, access codes, or hardware token devices ("Access Credentials") for your account or any other user account.
2. Provide unauthorized third parties, including family and friends, access to Rush information, IT resources, or facilities. This includes family and other household members when work is done at home.
3. Store Rush passwords in an insecure manner. This includes writing passwords on physical paper and storing them in a visible location, or creating a Word, Excel, or other electronic document containing passwords and storing that document on Rush file shares.

3.3 Data Protection

Do (Acceptable Use)

1. Store Rush documents in Rush-approved file storage locations like SharePoint or OneDrive.
2. Comply with data classification policies and handle information according to its level of confidentiality. See the *Information Classification Standard* for more on this.
3. Use Electronic Protected Health Information ("ePHI") in accordance with the Rush HIPAA Security Policy and policies related to patient privacy and security.
4. When your employment or association with Rush ends, return all classified information in your possession in accordance with the *Record Retention Policy*.
5. Promptly return all Rush-owned technology resources on request or during separation from Rush in accordance with the *Computer Hardware Policy and Standards* (D&IS).
6. Comply with the *Artificial Intelligence Policy* when using Artificial Intelligence tools and technology.

Don't (Unacceptable Use)

1. Share Rush data with unauthorized individuals or store data on non-standard platforms.
2. Use personal cloud content collaboration tools (e.g., Google Docs, Apple iCloud, or other online data exchanges) for storing or sharing Rush classified information.
3. Access, use, store, or disclose Rush classified information (or non-consensual images or videos) on devices not managed by Rush D&IS.

4. Input or upload any Rush classified information into public or unapproved Artificial Intelligence (AI) tools.
5. Provide information about, or lists of, people affiliated with Rush to parties outside of the Rush system.

3.4 Email and Communication

You are responsible for the work you create, including, but not limited to, emails, instant messages, videos, or information placed or posted on the internet.

Do (Acceptable Use)

1. Promptly report any external communications or correspondence you may receive relating to a cybersecurity incident or suspected data breach, including detections or alerts from antivirus software.
2. Use your Rush official email address(es) for business purposes only.
3. Report suspected phishing emails.

Don't (Unacceptable Use)

1. Use personal email to conduct Rush business.
2. Forward Rush classified information from your Rush email account to your personal email account or any email account outside the Rush system unless it is for authorized business purposes.
3. Open attachments or click links in emails from unexpected or unfamiliar sources.
4. Use Rush email accounts to conduct personal business or to create personal accounts (e.g., login accounts for shopping, dating, or social media websites).

3.5 Software and Applications

Do (Acceptable Use)

1. Use Rush-approved software and applications when conducting Rush business.

2. If you want to use an application not on the list of Rush-approved software, request review and approval from D&IS before installing, deploying, or using it on a Rush device.
3. Remember that you are responsible for the data you allow into Rush networks. If something looks sketchy, it probably is.
4. Conduct your personal online interactions (including banking and health care) on personal devices.

Don't (Unacceptable Use)

1. Introduce viruses, malware, or other harmful software into the Rush computing environment.
2. Conduct Rush business on unauthorized technology software, applications, devices, or cloud services. Unauthorized software or applications include, but are not limited to, free online websites or applications from the App Store or Google Play Store, such as artificial intelligence listening and note-taking software.

3.6 Rush Owned or Managed IT Devices and Assets

Do (Acceptable Use)

1. Report lost or stolen Rush-owned or managed IT assets to the D&IS Service Desk and Security Services.
2. Take responsibility for the physical security of Rush-owned or managed devices. Never leave devices unattended or visible when traveling or working outside your normal space.
3. Allow D&IS to patch and update IT devices and assets in your care.
4. Log off or activate the screen lock when you step away from your device.

Don't (Unacceptable Use)

1. Allow non-Rush people to use Rush-owned or managed IT assets.
2. Connect to the Rush guest network to bypass security controls, including accessing blocked websites.

3. Engage in activity that appears to be or is malicious (e.g., network scanning, circumventing authentication, or denying network services to any user). These activities may only be performed by members of the D&IS team with express permission from the Chief Information Security Officer, who will approve the scope and rules of any such actions in advance.

3.7 BYOD/ Personal Devices

When using personal devices to access Rush IT resources or conduct Rush business, users must ensure the security of their devices and the confidentiality, integrity, and availability of Rush data. Personal devices may be subject to security requirements such as password protection, encryption, antivirus software, and, in rare cases, device locking.

Rush is not responsible for any loss or damage to your device, or if it is stolen. However, if your personal device has Rush applications or data on it, and it gets lost or stolen, D&IS may remotely wipe that device of Rush data.

Work with D&IS to wipe all Rush data from your devices when you leave Rush.

Do (Acceptable Use)

1. Ensure all personal devices used for business are approved and compliant with Rush security policies.
2. Follow Rush security policies when using personal devices to conduct Rush business, which may require registration with D&IS.

Don't (Unacceptable Use)

1. Share personal devices with any other person while applications with access to Rush systems or data are open.
2. Use personal devices to text, share, or store classified information (e.g., ePHI, PII, financial information, sensitive Rush data, etc.).

Policy Title: Acceptable Use of Information Technology Resources Policy		**Policy Number:** N/A	
Document Owner: Kristin Parker		**Approver(s):** Michael Levinson	
Date Created: 10/20/2025	**Date Approved:** 10/20/2025	**Date Updated:** 11/24/2025	**Review Due:** 10/20/2026
Applies To: RUMC ☒ RMG ☒ ROPH ☒ RCMC ☒ RU ☒			

4. Monitoring

Accountability is one of our values, but it does happen that sometimes someone will violate that principle or one of our cybersecurity policies. Therefore, Rush reserves the right to monitor use of its technology resources to:

- Ensure compliance with policies
- Investigate security events
- Maintain system integrity

Rush may monitor, intercept, record, read, copy, and capture any electronic traffic, and may disclose material it finds to authorized personnel without additional notice to users.

5. Applicability

Regulatory Framework	Function, Category, or Clause	Control or Reference
NIST CSF	Roles, Responsibilities, and Authorities (GV.RR) Awareness and Training (PR.AT)	GV.RR-01, GV.RR-04, PR.AT-01
NIST 800-53	AC - Access Agreements AU - Rules of Behavior	PS-06, PL-04

6. Associated Documents

Document Type	Name of Document
Standard	IT 09.02 Auditing and Logging Standard

Policy Title: Acceptable Use of Information Technology Resources Policy		**Policy Number:** N/A	
Document Owner: Kristin Parker		**Approver(s):** Michael Levinson	
Date Created: 10/20/2025	**Date Approved:** 10/20/2025	**Date Updated:** 11/24/2025	**Review Due:** 10/20/2026
Applies To: RUMC ☒ RMG ☒ ROPH ☒ RCMC ☒ RU ☒			

Standard	IT 07.03 Encryption Standard
Standard	IT 01.01 Information Classification Standard
Standard	Information Security Risk Management Standard
Standard	IT 19.00 Asset Management and Lifecycle Policy
Standard	Computer Hardware Policy and Standards (D&IS)
Policy	HIPAA Privacy Policy
Policy	HR-A 01.00 Code of Conduct
Policy	Artificial Intelligence Policy
Policy	HIPAA Security Policy
Policy	Research Data - Access, Ownership and Retention
Policy	Social Media
Policy	Copyright Compliance

7. Disclaimer

Ownership: The Rush Information Security Department is the author and designated owner of this policy.

The Information Security department is responsible for overseeing and implementing this policy. Individuals who violate this policy will be subject to disciplinary actions up to and including termination as determined by Human Resources.

Exceptions to this Policy: Requests for exceptions to this policy's requirements must be managed in accordance with the requirements of the Information Security Risk Management Standard.

Policy Title: Acceptable Use of Information Technology Resources Policy		**Policy Number:** N/A	
Document Owner: Kristin Parker		**Approver(s):** Michael Levinson	
Date Created: 10/20/2025	**Date Approved:** 10/20/2025	**Date Updated:** 11/24/2025	**Review Due:** 10/20/2026
Applies To: RUMC ☒ RMG ☒ ROPH ☒ RCMC ☒ RU ☒			

Renewal & Review: Rush will review this policy annually to determine whether it continues to address current Rush requirements and regulatory compliance needs. Rush will update this policy to meet changes in the security and regulatory environment.

Approval: The Chief Information Security Officer or their delegate will review and approve this policy.

8. Revision History

Version	Date	Authors	Notes
1.0	August 2025	Julia Breaux, Susan Nuccio, Andrew Reeder, Kristin Parker, Enrique Escalante, Shelby Handrich Hwang, Lori Bysong	Refresh from the previous policy, IT 05.00 Acceptable Use of Information Technology Resources Policy. Updated with iCare Values.

9. Approval History

Version	Approval Date	Approved By	Title/ Role
1.0	24 November 2025	Michael Levinson	AVP Chief Information Security Officer