System Update Policy

Originator name:	Donald Macinnes
Section / Dept:	Information Compliance Unit
Implementation date:	TBA
Date of next review:	TBA
Related policies:	Data protection policy IT Acceptable Use Policy Information Security Policy Security Sensitive Research Policy
Policy history:	N/A

Version History

Version	Author	Revisions Made	Date
1	Donald Macinnes	First Draft	5 October 2018
2	Donald Macinnes	Revisions from Lorne Bozinoff included	8 September 2020

1	**Introduction**
	Forum Research Inc. will review, evaluate, and appropriately apply software patches in a timely manner. If patches cannot be applied in a timely manner due to hardware or software constraints, mitigating controls will be implemented based upon the results of a risk assessment. Forum Research Inc. will adhere to National Institute of Standards and Technology (NIST) guidance as set forth in Special Publication 800-40, Creating a Patch and Vulnerability Management Program, and any revised or updated successors.
1.1	**Rationale**
1.1.1	In order to ensure the security of our network and protect the company's data, all computers and network devices must be maintained at vendor supported levels and critical security patches must be applied in a timely manner consistent with an assessment of risk. This is a requirement of Forum's Information Technology Security Program, and industry best practice guidelines.
1.2	**Applicability of the Policy**
1.2.1	This policy covers all servers, workstations, network devices, operating systems (OS), applications, and other information assets for which vendors provide system patches or security updates.
1.3	**Equality Analysis**
1.3.1	TBA
1.4	**Definitions**
1.4.1	**Network Devices** - Any physical component that forms part of the underlying connectivity infrastructure for a network, such as a router, switch, hub, bridge, gateway, etc **Network Infrastructure** - Includes servers, network devices, and any other back-office equipment **Patch** - A fix to a known problem with an OS or software program. For the purposes of this document, the term "patch" will include software updates. **OS** - Operating System such as Windows, Mac, Linux **Risk Assessment** – An evaluation of the level of exposure to a vulnerability for which a patch has been issued **Update** – a new version of software providing enhanced functionality and/or bug fixes **Vendor** - Any organization or individual(s) that do business with the company
2	**Procedure**
2.1	**Pre-Patch Management**

2.1.1	Pre-patch Management: Patch Management and System Updates Policy 1. System administrators will use automated tools, where available, to create a detailed list of all currently installed software on workstations, servers, and other networked devices. A manual audit will be conducted on any system or device for which an automated tool is not available. 2. Systems and software will be evaluated to verify currency of patch and update levels and an analysis of vulnerabilities will be performed. 3. Specific guidelines for applying patches and updates will be developed and made available to system administrators.
2.2	**Patch Management**
2.2.1	1. Automated tools will scan for available patches and patch levels, which will be reviewed as specified in the Patch Application Guidelines. 2. Manual scans and reviews will be conducted on systems for which automated tools are not available. 3. An informal risk assessment will be performed within 2 business days of the receipt of notification of patches. If a determination regarding the applicability of the patch or mitigating controls cannot be made at that time a formal risk assessment will begin. 4. Vendor-supplied patch documentation will be reviewed in order to assure compatibility with all system components prior to being applied. 5. Where possible, patches will be successfully tested on non-production systems installed with the majority of critical applications/services prior to being loaded on production systems. 6. Successful backups of mission-critical systems will be verified prior to installation of patches and a mechanism for reverting to the patch levels in effect prior to patching will be identified. 7. Patches will be applied during an authorized maintenance window in cases where the patch application will cause a service interruption for mission-critical systems. 8. Patches will be prioritized and applied in accordance with Patch Application Guidelines. 9. Logs will be maintained for all system categories (servers, secure desktops, ASCI, switches, etc.) indicating which devices have been patched. System logs help record the status of systems and provide continuity among administrators. The log may be in paper or electronic form. Information to be recorded will include but is not limited to: date of action, administrator's name, patches and patch numbers that were installed, problems

	encountered, and the system administrator's remarks. 10. In the event that a system must be, reloaded, all relevant data on the current OS and patch level will be recorded. The system should be brought back to the patch levels in effect before reloading. 11. In the event that a patch will not be applied due to incompatibility or risk assumption, precautions to mitigate the risk of exploitation to the company network will be implemented and documented in the log.
3	**Governance Requirements**
3.1	**Roles & Responsibility**
3.1.1	1. Information Technology Staff are responsible for ensuring that information resources are maintained in compliance with SUNY Oneonta patch management policies and procedures. 2. Administrators of systems not managed by IT Staff are responsible for ensuring that their systems are maintained in compliance with SUNY Oneonta patch management policies and procedures (e.g.: departmental servers, utility devices, etc.). 3. The Information Technology Security Administrator is responsible for auditing information systems to ensure that they comply with SUNY Oneonta patch management policies and procedures.
3.2	**Implementation / Communication Plan**
3.2.1	The key elements of this policy which require communication to all staff are included in the IT Acceptable Use policy. No site wide communication of this policy is therefore required. The policy will be published on the company policies website.
3.3	**Exceptions to this Policy**
3.3.1	As this policy outlines the procedures to follow to undertake any form of patching and monitoring which means that, provided the appropriate conditions are in place, monitoring should be possible. No exceptions to the policy are envisaged.
3.4	**Supporting documentation**
3.4.1	N/A