

## GA 43. Operating System updates Policy

---

|                      |   |
|----------------------|---|
| Title:               | Antivirus Policy                                |
| Policy Number:       | GA 43 / 07.18                                   |
| Effective Date:      | July 24, 2018                                   |
| Approval and Review: | <b>Revised and approved on October 22, 2024</b> |
| Issuing Authority:   | VP for Development                              |

---

### 1. RATIONALE

---

RHU is committed to ensuring a secure computing environment and recognizes the need to prevent and manage IT vulnerabilities. A compromised computer threatens the integrity of the network and all computers connected to it. Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within university.

### 2. POLICY

---

The purpose of this policy is to ensure that all University-owned devices are proactively managed and patched with appropriate security updates

- All servers in data centers will be maintained with the latest security patches to their operating systems and key applications.
- All PC's are to be configured such that they schedule regular operating system updates as provided by the vendor (Windows updates).
- All patches that are medium/high severity or for non-critical systems must be installed soon.
- Any low priority patches will be installed on a case-by-case basis.
- All patches should be tested on development systems before being rolled out to production, where possible.
- All University-owned Windows based endpoints are to have critical operating system and key application patches installed within 30 days of release from the vendor.

### 3. RELATED DOCUMENTS

---

- > IT Manual