



RNDC IT EQUIPMENT & SOFTWARE POLICY

Effective June 1, 2022



TABLE OF CONTENTS

1. OVERVIEW
2. STANDARD IT EQUIPMENT
3. NON-STANDARD EQUIPMENT REQUESTS
4. HARDWARE STANDARDS REVIEW CYCLE
5. AVERAGE LIFECYCLE OF COMMON HARDWARE
6. ASSIGNMENT OF IT EQUIPMENT
7. RETURNING COMPANY IT EQUIPMENT
8. COMPANY'S SOFTWARE POLICY
9. SOFTWARE MANAGEMENT POLICY & EXCEPTIONS
10. SOFTWARE AUDIT CONTROLS



1. OVERVIEW

This document informs associates about policies regarding IT Hardware, Software, and the support lifecycle. The goal is to improve IT efficiency, reduce exposure to risk, and deliver value to the business while reducing costs. This is an evolving policy and will be updated as needed.

Hardware: in the context of this policy, is defined as desktops, laptops, notebooks, mobile devices (including but not limited to iPads, MS Surfaces, MiFi's, and smartphones), printers, projectors, scanners, monitors, or any variation of computer equipment that the Company uses for business purposes, except for the copier fleet.

Software: in the context of this policy, is defined as the default software installed from the manufacturer as well as approved business software purchased by RNDC for use in specific job tasks in conducting business. All software is governed by the licensing agreement and will be managed by the Asset Administrator and the IT teams.

2. STANDARD IT EQUIPMENT

RNDC supports a standardized computer environment to control overall support and equipment purchase costs. The standard computer bundle (Desktop PC, Laptop, or Tablet) is composed of higher-end business models that meet most RNDC business needs.

The following equipment is provided to all Full-time associates. Some exceptions may be made for remote work and role specific needs.

- One standard laptop with built-in webcam and microphone
- Desktop PC and Tablets are specific to job requirement
- A docking station (Laptop only)
- Two external monitors
- Mouse & Keyboard combo
- Wired Headset

If additional and/or alternative equipment is required, exceptions may be made on a case-by-case basis. If you feel you require an exception, please follow the Non-standard Equipment Request process below.

Please note all IT/AV-related purchases must be arranged through Procurement.

Purchases made by individuals using personal debit/credit cards will not be reimbursed unless approved by the VP of Indirect Procurement.



Standard peripheral items (mouse, keyboard, headset, device cases, etc.) provided have been paid for by the company. If a different model or upgrade item is needed the associate should purchase at their own expense. The company provides standard items as outlined in this document. Items such as mouse pads, monitor stands, laptop stands, laptop coolers, device cases/ backpacks, and specific home use items for remote/ hybrid work can be purchase at the associate's expense with no reimbursement.

3. NON-STANDARD EQUIPMENT REQUESTS

A request for non-standard IT Equipment, which includes both Windows and MACs, must be accompanied by an explanation of the business need. If the non-standard hardware is approved, Procurement will acquire the requested equipment and arrange deployment in coordination with the Deskside Support team.

NON-STANDARD EQUIPMENT REQUESTS REVIEW AND PURCHASE PROCESS

- **Request:** The associate submits a request in ServiceNow using the Non-Catalog Request form to Procurement and provides a business justification for the exception request.
- **Evaluation:** The request is evaluated to determine whether standard equipment will meet the business need or whether non-standard equipment is required. Each request will be considered on a case-by-case basis in conjunction with the business need.
 - o If there is an approved business need for non-standard equipment IT will then evaluate the software being used and select the suitable hardware. The Procurement team will purchase the equipment.
 - o All computer equipment is solely property of RNDC and is returned to the local IT Deskside Support for re-use or disposition when no longer needed by the associate it was purchased for.
 - o If there is no business need for the non-standard equipment, or it does not meet security standards, the Procurement team will communicate the reason to the department and suggest use of standard equipment.
 - o At no time is an associate permitted to purchase their own IT Equipment for use on company systems, nor will they be permitted to expense purchase of non-standard equipment.

4. HARDWARE STANDARDS REVIEW CYCLE

Hardware standards will be reviewed on a regular basis to, (1) align with department and business strategic framework; (2) ensure that support has not ended on the device; (3) determine or modify the end-of-life dates for Company support; (4) verify pricing; and (5) to update the model version if necessary.



5. AVERAGE LIFECYCLE OF COMMON HARDWARE

- Desktop PC: 5 Years
- Laptop PC: 5 Years
- Tablets: 5 Years
- Smartphones: 4 Years

6. ASSIGNMENT OF IT EQUIPMENT

All Company IT Equipment will be assigned to the associate within the Asset Management system for reporting and tracking of all company assets. Associates are responsible for all IT Equipment assigned to them.

7. RETURNING COMPANY IT EQUIPMENT

All Associates are responsible for all RNDC property, materials, or written information issued to them or in their possession or control.

All RNDC property must be returned on or before the last day of work. Where permitted by applicable laws, RNDC may withhold from an associate's check or final paycheck the cost of any items that are not returned when required. RNDC may also take all action deemed appropriate to recover or protect its property.

8. COMPANY'S SOFTWARE POLICY

If the associate wants to install software on Company computers, s/he must contact the IT Department and request to have the software installed. Associates are prohibited from installing any software on any Company technical resource without the express prior written permission from the IT Department.

Involving the IT Department ensures that the Company can manage the software on Company systems, prevent the introduction of computer viruses, and meet its obligations under any applicable software licenses and copyright laws. Computer software is protected from unauthorized copying and use by federal and state law; unauthorized copying or use of computer software exposes the Company, and the individual employee, to substantial fines and exposes the individual employee to imprisonment. Therefore, associates may not load personal software onto the Company's computer system and may not copy software from the Company for personal use. Any software loaded in violation of this policy will need to be validated to prove ownership and that it has not been pirated or copied in violation of copyright laws. It may also be removed.



9. SOFTWARE MANAGEMENT POLICY & EXCEPTIONS

The standardized software policy offers better supportability, a more consistent operating experience for users and is one component used to help protect the security of RNDC resources. The Cyber Security team is tasked with ensuring that only approved applications are used on computing devices within the organization. The policy is designed to protect RNDC by requiring all employees to only run software application programs on deemed safe and standard by the Company. This helps to ensure all applications in use meet RNDC security, functional, and support criteria.

The Cyber Security Team shall prepare and maintain a list of software applications that are approved for general use on company devices. Only approved software applications are allowed to access RNDC networks and information resources. Under no circumstances shall associates use programs that are not on the approved list of software applications. Associates who introduce a security issue by installing and running an unapproved program risk disciplinary action.

Should an associate need access to a software that does not appear on the approved list for their work, they must submit a justification request to the Cyber Security Team to evaluate the application and request. This process applies to licensed applications, shareware, freeware, trial programs, and all other software installed on the user's business computing assets. Exceptions are reviewed on a case-by-case basis and documented.

As with IT Equipment, no associate is authorized to purchase their own software and expense it.

10. SOFTWARE AUDIT CONTROLS

The Cyber Security team and Asset Management shall conduct periodic software audits on all company assets to determine usage rates, compliance, and end-of-life applications. The company reserves the right to remove applications that are not in use, out of compliance, and end-of-life from company deployed assets.