



## Risk Management for Replication Devices

A replication device (RD) is any device that reproduces (e.g., copies, prints, scans) documents, images, or objects from an electronic or physical source. For the purposes of this NISTIR, RDs include copiers, printers, three-dimensional (3D) printers, scanners, 3D scanners, as well as multifunction machines when used as a copier, printer, or scanner. RDs in use within organizations run the gamut in terms of age and functionality. Older, single-function devices may have no internal, nonvolatile storage and cannot be networked. Other devices may provide a variety of functions, be network-connected, run commercially available operating systems, contain internal, nonvolatile storage, and contain embedded internal print servers and web server capability. In between the two extremes, there may be RDs with network and/or storage functionality but no discernable means to configure them securely. Additionally, many organizations may not have an accurate inventory of RDs or recognize what functionality each device possesses, especially with respect to information (data) storage, processing, and transmission.

Managing the risks associated with RDs requires a basic understanding of threats, vulnerabilities, potential impact and likelihood of an event, and the identification and implementation of countermeasures or mitigation strategies. This publication provides guidance on protecting the confidentiality, integrity, and availability of information processed, stored, or transmitted on RDs.

The attached zip file includes:

- Intro Page.pdf
- Terms and Conditions.pdf
- Risk Mgmt Replication Devices.pdf