YU ITS Administration, Faculty & Staff Handbook

Contacting Support:

ITS Help Desk, helpdesk@yu.edu, 800-337-2975 or 646-592-4357, Teams dial 4357

[Updated 01/19/2024]

Revision History

Name	Date	Reason For Changes	Version	Approved
ITS	02/10/2022	Inherited Draft	2.2	February 2022
Jorge Warman, ITS	01/19/2024	Added password length and complexity detail	3.0	01/19/2024

Enforcement

Violations of the policies, processes, standards and guidance in this handbook or any other policies, plans, standards, or procedures intended to secure and protect systems and information from unauthorized access or use, alteration, deletion or transmission may result in temporary or permanent loss of system privileges and in disciplinary action up to and including termination.

Table of Contents

Purpose

Yeshiva University ("**YU**" or the "**University**") provides various technology resources, including computers, Internet access, email, and telephones (including smartphones), to the University community to facilitate the exchange of ideas and information, and to aid in the University's communications and work-related research by the University community. Use of these resources is governed by the University's policies, including this Handbook, and applicable laws.

All Users (defined below) are required to read and understand this Handbook and the policies contained herein and to sign the User Acknowledgement at the end of this document. Policy violations may have serious consequences for a User's access to resources and their University career.

The University reserves the right to revise and modify the policies contained in this Handbook in its sole discretion. Questions concerning this Handbook and the policies contained herein should be addressed to the University's Information Security Administrator at infosec@yu.edu. Any misuse of University computers or computing resources, or evidence of intrusions or tampering, should be promptly reported by email to abuse@yu.edu. Nothing in this Handbook creates any expectation of privacy or alters any employment relationship.

Definitions

Term	Definition
Copyright	Legal protection for original works of authorship that are fixed in a tangible means of expression. Text (including email and web information), graphics, art, photographs, music, film, and software are examples of types of work that may be protected by copyright
Document	Any letter, memorandum, tape recording, electronic mail, electronic document, note, or written communication
Incidental Personal Use	Occasional, non-commercial personal use that takes place outside of normal work hours at negligible cost to the University and does not interfere with the University's needs or operations or a User's job

ITS	The University's Information Technology Services Department
Peer-to-Peer (P2P)	Software, services, and protocols that are commonly referred to as "peer-to-peer" or "P2P," such as BitTorrent. P2P includes, without limitation, software that enables the sharing of files among a network of computers without a need for centralized storage of such files
Personal Information	Information that can be used to identify an individual. Personal Information includes an individual's name, work or home address, email address, telephone or facsimile number, SSN, or other government identification number, employment information and background information, financial information, medical or health information (such as an individual's health insurance identification number or condition), account numbers, certificate or license numbers, vehicle identifiers and serial numbers (including license plate numbers), device identifiers and serial numbers, biometric identifiers (including finger and voice prints), and photographs. Personal Information may relate to any individual, including University students, administration, faculty, staff, officers, trustees, committee members, overseers, consultants, and individuals associated with students, faculty, staff, consultants, vendors and other third parties
Technology Resources	Consists of all University-owned personal computers and workstations, including notebook and laptop computers; peripheral equipment such as monitors, keyboards, mouse, printers, telephone equipment; smartphones; computer software applications and associated files and data; direct (wired and wireless) and remote access to the University's network; and access to outside sources of information such as the Internet
Cloud Service Provider	An entity that issues or registers subscriber authenticators and issues electronic credentials to

	subscribers to allow access to use a service or application
University Community	All University administration, faculty, staff, and students
User(s)	All University administration, faculty, and staff (including student employees), as well as volunteers and interns, with access to Technology Resources
Yeshiva University Information	Any information that is collected, used, or maintained by the University
Controlled Information	Information that requires protection; information that meets the definitions of Restricted Information and Internal Information
Restricted Information	Information whose loss, corruption, or unauthorized disclosure would cause severe personal, financial, or reputational harm to the organization, organization staff or the constituents/people we serve; information whose protection is required by law, regulation, or university-wide policy
Internal Information	Information whose loss, corruption, or unauthorized disclosure would likely cause limited personal, financial, or reputational harm to the organization, organization staff or the constituents/people we serve
Public Information	Information whose loss, corruption, or unauthorized disclosure would cause minimal or no personal, financial, or reputational harm to the organization, organization staff or the constituents/people we serve

Policy

Introduction

All University faculty and staff with access to Technology Resources (Users) are required to read and understand this Handbook and the policies contained herein. All Users with access to Yeshiva University Information or Technology Resources must comply with the University's policies and procedures relating to information security. Policy violations may have serious consequences.

As a condition of a continued working relationship with the University, each User must:

- read and comply with all University policies, including those contained in this Handbook; and
- annually acknowledge that they have received a copy of this Handbook and agree to comply with the policies contained herein.

All information stored, transmitted, or handled by the Technology Resources is the property of the University. Subject to applicable law, authorized University personnel may review and monitor this information at any time without the User's permission. In general, any review and monitoring will be conducted in furtherance of the University's academic and business pursuits and, to the extent deemed appropriate by a senior ITS administrator, in consultation with the University's Office of the General Counsel or outside counsel. Users should harbor no assumption of privacy.

Using Technology Resources

All Technology Resources under the control of YU are provided for the furtherance of the University's academic and business pursuits. YU extends access privileges to members of the University community and expects them to comply with all applicable University policies and applicable state and federal laws in accessing these resources.

No User may use the Technology Resources for the conduct of non-University business, including private solicitations, or political or commercial activities. In addition, Users may not use the Technology Resources to commit any illegal act; or harass an individual or organization.

Notwithstanding the above, Users may use the Technology Resources for Incidental Personal Use (so long as they are in compliance with other applicable University policies). Examples of Incidental Personal Use include using the Technology Resources to:

- prepare and store incidental personal data (such as personal calendars, personal address lists, personal email, personal Internet links and similar incidental

personal data) in a reasonable manner, provided such use does not conflict with any purpose or need of the University.

- send and receive necessary personal communications through email (to the extent not prohibited by the University's Email Policy), however, all communication used by a YU-owned email account is owned by YU. Users have no expectation of privacy using YU email or Technology Resources.
- use computers and smartphones to conduct personal transactions and retrieve information of personal interest from the Internet, provided such activity excludes prohibited activity (listed in the Internet Access and Use Policy).
- use the telephone system for brief and necessary personal calls.
- participate in University-sponsored Internet communities within defined guidelines.

The following practices are examples that do not qualify as Incidental Personal Use and are not appropriate unless required for the User's position at the University:

- viewing, sending or drafting gross, indecent or sexually oriented materials.
- visiting gambling sites.
- visiting illegal drug-oriented sites.

The University assumes no liability for loss, damage, destruction, alteration, disclosure or misuse of any personal data or communications transmitted over or stored on the Technology Resources. YU accepts no responsibility or liability for the loss or non-delivery of any personal email communication. The University reserves the right to suspend or limit privileges as required in its sole discretion to protect and operate the Technology Resources.

Privacy

User Privacy

Subject to applicable law, all information created, sent, or received via the Technology Resources may be reviewed and monitored by authorized University personnel at any time without User permission. In general, any review and monitoring will be conducted in furtherance of the University's academic and business pursuits and, to the extent deemed appropriate by a senior ITS administrator, in consultation with the University's Office of the General Counsel or outside counsel. Examples of reasons to review and monitor information, files and messages on the Technology Resources include, but are not limited to, determining compliance with University policies, answering a subpoena or court order, investigating misconduct, or locating information necessary for its operations.

Users do not have a personal privacy right in any material created, received, saved, or sent by the Technology Resources. The granting of a password does not confer any right of privacy upon any User. Users should assume that all documents created or saved on the Technology Resources are the University's property.

Users who use the Technology Resources to create or maintain personal information or messages have no right of privacy with respect to those messages or information. The University provides the Technology Resources only to further its own academic and business aims. All Technology Resources and all information, documents and messages stored on the Technology Resources should be related to the business of the University (except as expressly provided in this Handbook).

The best way to guarantee the privacy of personal information is not to store or transmit it on the Technology Resources.

Yeshiva University Privacy

The University seeks to ensure that information and messages stored and transmitted on the Technology Resources are safe from unauthorized use or examination. Users should not, however, assume that information or messages stored or transmitted on the Technology Resources are safe from unauthorized access. Users should comply with the Related Policies listed below to enhance the privacy of Yeshiva University Information:

Related Policies in this Handbook:
Information Security & Technology Resources
Internet Access and Use
Electronic Mail (Email)
ITS Encryption Policy

Installation and Use of Software

The loading and unloading of any software package onto or off a University-owned system must be properly licensed and compatible with the University's network. It is YU's policy that all software on the Technology Resources is officially licensed to YU and approved by ITS. The User loading onto, or otherwise utilizing software on, the Technology Resources is responsible for ensuring that the software is properly licensed and approved. Further, all software purchased by, licensed by, or created by the University is the exclusive property of the University. Without the prior written authorization of an authorized representative of ITS, Users may not:

- Install University-owned or licensed software on any non-University owned computer equipment; or

- Provide copies of University-owned or licensed software to anyone.

Related Policies in this Handbook:
Use of Copyrighted Material
P2P File-Sharing Policy

Use of Copyrighted Materia

All members of the University community are responsible for complying with copyright laws (and other intellectual property and proprietary rights). In general, copyright laws protect and grant exclusive rights to authors of published or unpublished original works that have been recorded in tangible form, including literary works, musical works, dramatic works, pantomimes and choreographic works, pictorial, graphic, and sculptural works, motion pictures and other audiovisual works, sound recordings and architectural works.

In compliance with copyright laws and this Handbook, Users may not:

- copy, distribute, download or upload copyrighted material to and from the Internet in a manner that violates the owner's copyright protections;
- copy, distribute, download or upload copyrighted material from original media in a manner that violates the owner's copyright protections; or
- use P2P file-sharing software on the University's network except as authorized by ITS in writing.

All Users are expected to cooperate with ITS to ensure that all copyrighted material found or utilized on the Technology Resources is properly licensed. For more information on the University's policies regarding copyrights, please see the Yeshiva University Digital Millennium Copyright Act (DMCA) policy on the University's website and also available from ITS. A User's unauthorized distribution of copyrighted material, including P2P file-sharing, may subject the User to civil or criminal liability, as well as disciplinary action

Related Policies in this Handbook:
Installation and Use of Software
P2P File-Sharing Policy
Internet Access and Use

P2P File-Sharing Policy

ITS is responsible for the design, throughput, availability, and overall health of the University's network. Peer-to-Peer (P2P) file-sharing software is used to connect computers directly to other computers in order to transfer files between the systems directly, without

the need for centralized storage of those files (for example, on centralized servers). P2P software, when abused, can saturate an entire network and leave some or all of its users with poor to non-existent performance. Additionally, P2P software is frequently used for the transfer of copyrighted materials (such as music and movies) in violation of the Yeshiva University Digital Millennium Copyright Act (DMCA) policy.

To prevent any type of abuse or infringement (whether accidental or intentional), no P2P software may be used on or in connection with the Technology Resources, and the Technology Resources may not be used for any type of P2P file-sharing or similar activities. Exceptions can be made only with the express prior authorization of ITS, in ITS' discretion (see below).

Possible Exceptions—Authorization for Use of P2P Software

As noted above, exceptions for specific uses of P2P software may be made for specific Users (for example, if a User's work requires the use of a specific item of P2P software). Such exceptions may be made by ITS in its sole discretion. A request for such an exception may be made by submitting a ticket to the ITS Help Desk. As an example, a P2P application such as BitTorrent may have specific value for a particular type of work, such as the exchange of scientific information in connection with a particular project, and therefore a particular User may request that an exception be made.

- ITS reserves the right, in its sole discretion, to authorize use of P2P software on a per-User, case-by-case basis, when provided with specific, written purposes directly related to, or in support of, the academic, research or administrative activities of the University.
- Permission to use P2P software may be revoked at the discretion of ITS. This includes, but is not limited to, revocation for one or more of the following reasons: service abuse; degradation of the performance of the University network; and use for purposes other than University business or the specific purposes for which the exception was granted.

ITS reserves the right to periodically review Users' use of P2P software and activities that have been permitted pursuant to such exceptions.

User Responsibility

- Users must educate themselves on P2P software through the resources provided on the ITS website.
- Users must not knowingly download, install, or use P2P software without ITS' authorization. This includes a User configuring any resource attached to the YU network (including their computer) so that files stored on or in connection with such resource are available to other Users or third parties using P2P software or protocols.

- Users must remove any P2P software that is discovered on any resource attached to the YU network, including personal property, unless granted specific permission by ITS in advance.

Enforcement of P2P Policies

To prevent the use of P2P applications, ITS blocks well-known "ports" that are used by P2P software and protocols; however, some P2P applications are still able to negotiate connections on other, dynamic ports. If ITS detects a system engaging in P2P activity, ITS has the right to block all such activity and/or to disconnect such system. Continued unauthorized use of P2P software over YU's network may result in disciplinary action or termination of access to Technology Resources.

Related Policies in this Handbook:
Installation and Use of Software
Use of Copyrighted Material
Internet Access and Use

Information Security & Technology Resources

All Users must properly safeguard and handle Yeshiva University Information, regardless of its form (*e.g.*, electronic records), as more fully set forth below. Users are responsible for preventing unauthorized access to, and protecting the security and confidentiality of, Yeshiva University Information.

Authorized Access

Users may not allow any person to access, in any manner, YU-owned computer equipment unless that person is specifically authorized to access such equipment.

Users should not disclose their YU credentials to anyone. There are no exceptions, and the User will be responsible for the actions of such other person. If a legal, harassment, or other complaint or charge is made against a specific YU credential, the owner of those credentials is liable.

A common method for hackers to gain access to computer networks is for the hacker to impersonate a member of ITS. The hacker will call a User with a story that they need the User's login ID and password. **Members of ITS will never call a User and ask for a login ID and password. NEVER!**

The fact that information stored on the Technology Resources is *accessible* does not necessarily mean that access to it is *authorized*. Even when physically able to, Users may not access any

information other than that which they are specifically authorized to access and which is necessary for the performance of their assigned duties.

Data Retention

It is recommended that each User consult with ITS and take such action as they deem reasonably appropriate to ensure that their computer files are properly backed up. All costs and expenses so incurred shall be subject to customary University approval.

The guidelines for the retention of University records are set forth in the Record Retention Policy found on the Office of the General Counsel website.

Related Policies in this Handbook:
Protection of Confidential Information and Personal Information
Password Policy
See also: Record Retention Policy.

Protection and Handling Restricted Information and Internal Information

YU is dedicated to protect the confidentiality and integrity of the information collected, processed, stored, or transmitted by YU personnel and YU systems. While working or studying at the University, Users may create, discover, use, access, receive or otherwise handle Restricted Information and Internal Information. No matter what a User's position or role at the University, every User has an obligation to safeguard Restricted Information and Internal Information.

All Users must properly handle the Restricted Information and Internal Information that they collect, process, store, or transmit in the course of business. This obligation includes:

- preventing unauthorized access to, and protecting the security and confidentiality of, Restricted Information and Internal Information;
- only collecting, accessing, using, maintaining, transmitting or disclosing the minimum amount of Restricted Information and Internal Information that is necessary and relevant to perform the User's job responsibilities;
- only removing Restricted Information and Internal Information from the University's offices when it is necessary and relevant to perform job responsibilities, or otherwise for allowable business purposes, and then only if it is password-protected and/or encrypted as described below;
- not using Restricted Information and/or Internal Information for unauthorized purposes and not permitting them to be used for unauthorized purposes;
- properly disposing of Restricted Information and/or Internal Information in a manner that is commensurate with the degree of risk posed by any disclosure of such information (*e.g.*, ensuring that SSNs are obscured to make them

unreadable, such as by wiping or shredding electronic media that contain SSNs); and
- notifying abuse@yu.edu if a User believes electronic records containing Restricted Information and/or Internal Information has been obtained or accessed by an unauthorized person.

Each User's obligation to safeguard electronic records containing Restricted Information and Internal Information extends to all situations in which a User may handle such information, including when the User is working remotely or otherwise away from the University's offices.

In addition, Restricted Information should not be stored on portable or removable devices, including laptops, unencrypted USB drives, unencrypted removable drives or portable media (*e.g.*, CDs and DVDs). If there is a business purpose to store Restricted Information on portable or removable devices, the User must consult with ITS to ensure the Restricted Information is encrypted and/or password protected as may be required by applicable law.

Restricted Information and Internal Information should not be stored using public Internet storage, including "cloud service providers". Users must use YU-owned or YU-licensed cloud services.

Restricted Information and Internal Information may not be transmitted, by any means, to third parties unless the following conditions are met:

- The transmittal is required for an allowable YU business purpose;
- The Restricted Information and Internal Information is encrypted following the ITS Encryption policy;
- The transmittal text includes a warning to the recipient that the material contains Restricted Information and/or Internal Information, and is the property of YU; and
- With respect to Restricted Information, the transmittal text must also include a specific statement of why the recipient is receiving it, what they may do with the information, and to whom, if anyone, they may disclose it.

As may be requested by the University, Users should provide authorized personnel of the University with access to any such encrypted or password-protected information.

Related Policies in this Handbook:
Technology Resources and Data Disposal
Remote Access
Work Outside of Yeshiva University's Premises
Laptops and Portable Devices
See also: ITS Encryption Policy

Physical Security of Technology Resources

Users must ensure that all Technology Resources (desktop computers, monitors, laptop computers, printers, phones, etc.) that are assigned to or regularly used by them are maintained and used by them in a manner consistent with their function and such that the possibility of damage and/or loss is minimized.

Computer equipment (other than laptops and other portable data equipment supplied by the University for a User's use outside of the University's premises) belonging to the University or maintained by ITS may not be removed from the University's premises without the prior written authorization of an authorized representative of ITS. Without the prior written authorization of an authorized representative of ITS, Users may not modify the University's computer equipment in any manner including, but not limited to, attaching external disk drives, external hard drives, changing the amount of memory in the computer, and attaching/installing any peripheral device, including wireless routers. Only modifications determined by ITS to be necessary for business or academic purposes will be authorized.

If a User connects their personal computer equipment to the Technology Resources, the User is responsible for the security of that equipment. Any misuse by a User of the Technology Resources, whether intentional, negligent, or otherwise, may result in the University denying that User access to the Technology Resources.

All Technology Resources must be:

- located in physically secure locations appropriate to the sensitivity of the resource; and
- placed in controlled and protected environments such that their purpose, functionality, or effectiveness is not placed in jeopardy, including, for example: placing file servers and routers outside of YU's general computer centers in locked closets; and storing all master copies of software in secure containers.

Related Policies in this Handbook:
Technology Resources and Data Disposal
Laptops and Portable Devices
See also: Bring Your Own Device (BYOD) Policy

Electronic Access Controls

Except with prior authorization from ITS, a User may not:

- test or attempt to compromise internal and preventive controls of any Technology Resource, such as system configuration files or antivirus parameters; or

- exploit vulnerabilities in the security of any Technology Resource for any reason, including, but not limited to:
    - damaging systems or information;
    - obtaining resources beyond those they have been authorized to obtain;
    - taking resources away from other Users; or
    - gaining access to Technology Resources for which proper authorization has not been granted.

Any misuse of University computers or computing resources, or evidence of intrusions or tampering, should be promptly reported by email to abuse@yu.edu.

All University-owned computers should have personal firewall software installed. Users may not modify this software; it is to remain activated and set to the highest protection status possible that supports business purposes at all times. An authorized representative of ITS will ensure that the software is updated as appropriate.

For systems and devices owned or otherwise controlled by the University, ITS will ensure that all security updates for operating systems, web browsers, server applications, and email clients are installed in a timely manner.

For systems and devices that are not owned or otherwise controlled by the University but are authorized to process YU's data and/or attached to the YU network, the User must ensure that all security updates for operating systems, web browsers, server applications, and email clients are installed in a timely manner.

Users should also take other precautions to protect their own personal computers:

- Use password-protected screensavers.
- Do not install any P2P software.
- Ensure that the computer is not configured to allow other devices' unauthorized access to YU's networks.
- Only use the YU user ID and password on authorized YU applications and sites. Never reuse the YU password on non-YU applications and platforms.

Related Policies in this Handbook:
Password Policy
Anti-Virus Protection
See also: Network Accessible Use Policy
See also: Bring Your Own Device (BYOD) Policy
See also: ITS Encryption Policy

Password Policy

Users must comply with all applicable guidelines promulgated from time to time by ITS in selecting passwords (including, without limitation, the length of the password). In accordance with industry standards, Users must choose passwords that cannot be easily guessed. In addition, passwords should not be related to a User's job or personal life. For example, a car license plate number, a spouse's name, or an address should not be used. Moreover, passwords also should not be words found in the dictionary, and proper names, places and slang should not be used.

Users should not construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example,
Users should not employ passwords like "X21JAN" in January or "X34FEB" in February.

Users should not use their Social Security numbers as passwords or any number derived from them, such as the last four digits of their Social Security number.

All User-chosen passwords must contain at least 12 characters with matching 3 of the following characteristics:

- numbers (0 to 9);
- upper case alpha characters (e.g., A or Z);
- lower-case alpha characters (e.g., a or z); and
- a special character (e.g. ' - ! " # $ % & ( ) * , . / : ; ? @ [ ] ^ _ ` { | } ~ + < = >)

Users should not construct passwords that are identical or substantially similar to passwords that they have previously utilized.

Different system accounts should have different passwords. User IDs and/or passwords must not be written down and not kept within the general area of the computer. Users may not utilize internal passwords or substantially similar passwords on external systems (*i.e.*, websites, web-based email, etc.).

A User must promptly change their password if the password is suspected of being disclosed or known to have been disclosed to another individual.

Related Policies in this Handbook:
Information Security & Technology Resources
Electronic Access Controls

Anti-Virus Protection

All computers, including a User's personal computer(s), that connect to the Technology Resources must have anti-virus and anti-spyware/malware software correctly installed, configured, activated, and updated with the latest version of virus definitions prior to use. This software is to remain activated (without User modification) with the most up-to-date virus definitions files at all times. An authorized representative of ITS will ensure that the software is updated as appropriate on University-owned Technology Resources. This will be accomplished wherever possible by using the approved, centrally administered anti-virus software and by configuring these systems to automatically receive the most current updates from a central server.

A User should notify the ITS Help Desk if the antivirus protection software is not working or if a device becomes infected with a virus. If a User suspects there is a virus on Technology Resources, the User should immediately stop using the computer, note the symptoms, and call the ITS Help Desk.

If a computer becomes infected with a virus or other form of malicious code, ITS will determine whether the computer must be disconnected from the University network until the infection has been removed and, in the case of a University computer, assist the User in removing the virus. ITS will endeavor to promptly notify the User of such action.

Users may not intentionally write, generate, compile, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of any computer's memory file system or software.

A User should use the Internet in a responsible manner and should avoid browsing or accessing inappropriate sites, and further should avoid opening attachments/files or clicking links in unknown/unexpected emails, that might expose their computer and, consequently, the Technology Resources, to viruses and similar threats.

Related Policies in this Handbook:
Electronic Access Controls

Reports of Lost Equipment or Potential Security Breaches

Users who suspect the loss or theft of any electronic equipment or any breach of the confidentiality or security of Confidential Information or Personal Information, must immediately contact the ITS Help Desk. Users may also send an email directed to abuse@yu.edu and infosec@yu.edu to report the loss, theft, or breach.

Smartphones may contain Confidential Information and Personal Information in the form of the University's internal contact list or in email messages and their attachments. Users should call

the ITS Help Desk immediately if a smartphone (or any Technology Resource) is lost or stolen. The unit's data will be wirelessly erased to minimize the risk of disclosure.

Related Policies in this Handbook:
Information Security & Technology Resources
Physical Security of Technology Resources
Laptops and Portable Devices

Technology Resources and Data Disposal

Information of a sensitive nature that is discarded inappropriately may fall into the wrong hands. Accordingly, all Technology Resources to be discarded that contains Confidential Information or Personal Information (in whole or part) must be properly destroyed and cannot simply be given away or deleted. Electronic media containing Confidential Information or Personal Information must be erased or destroyed to render them unreadable.

Therefore, Users may not dispose/discard/destroy Technology Resources or electronic media but must give it to ITS. **Only ITS** is authorized to dispose/discard/destroy Technology Resources and electronic media of the University.

Data on all University-owned electronic media, such as disk drives, tapes, CD-ROMs, flash memory, etc., must be destroyed prior to disposition, either by destruction of the media or destruction of the data which ensures the data cannot be recovered. An authorized representative of ITS will ensure that data on all electronic media to be discarded will have all Confidential Information and Personal Information thoroughly removed from it or securely and permanently disabled. All hardware must be disposed of through approved electronic equipment recyclers.

Moreover, Users shall not repair Technology Resources themselves, but must give to ITS, and ITS will have all Confidential Information and Personal Information thoroughly removed from it or securely and permanently disabled before being sent to a third party for repair.

Note Regarding Deleted Information

Deleting information, Documents or messages does not mean that the information, Documents or messages are really gone. Any information kept on the Technology Resources may be electronically recalled or reconstructed, regardless of whether it may have been "deleted" by a User. Because there are backups on tape of all files and messages, and because of the way in which computers reuse file storage space, files and messages may exist that are thought to have been deleted.

All Users should exercise care in what information or statements they create in electronic form to avoid potential embarrassment or legal liability for themselves or the University.

Related Policies in this Handbook:
Information Security & Technology Resources
Document Retention

Remote Access

Remote access connection to the University's network is allowed only through University-approved remote access technologies. All remotely connected devices must adhere to the University's anti-virus and security policies.

A User of a remote connection must:

- follow all University policies and procedures related to remote access;
- use a machine that has up-to-date anti-virus software running;
- not allow any File sharing or peer-to-peer program to be downloaded or running on the machine used to connect remotely, except where needed for University-support purposes; and
- report any observed or suspected violations of University policies and procedures related to remote access to the network.

Related Policies in this Handbook:
Information Security & Technology Resources
Anti-Virus Protection
Work Outside of Yeshiva University's Premises
Laptops and Portable Devices
See also: HR Remote Work Policy

Work Outside of Yeshiva University's Premises

When working outside of YU's premises, each User must:

- take steps at all times to protect YU's hardware, software and Information from theft, damage and misuse and unauthorized access or acquisition; and
- only keep, access and transmit records containing Confidential Information or Personal Information when such Information is necessary in order for the employee to perform their job responsibilities outside of University premises.

Related Policies in this Handbook:

Information Security & Technology Resources
Physical Security of Technology Resources
Remote Access
Laptops and Portable Devices
See also: HR Remote Work Policy

Laptops and Portable Devices

Physical Security

Users are responsible for their University-owned laptops and other portable devices s. Users should never leave a laptop or other portable device unattended, even for a few minutes, particularly in public places, such as at airports or on a train. In addition, laptops should not be checked as or with luggage on airplanes.

Automatic screen locking mechanisms and boot passwords should be used where possible.

Technical Security

University-owned laptops and portable devices should be password-protected with device lockout set for a minimum of 15 minutes. Data encryption should also be used where technically possible for all laptops and portable devices.

Each User who has been provided a University laptop or other portable device must:

- avoid placing Highly Sensitive Information on any laptop or portable device, unless the device is encrypted;
- minimize the amount of Confidential Information and Personal Information on the laptop or portable device to the amount reasonably necessary to perform the User's job duties;
- not use any option that "remembers" passwords;
- switch off the laptop or portable device when not in use;
- not tamper with anti-virus software and other security tools installed on the laptop or portable device; and
- never store passwords for any Technology Resource on the laptop or portable device.

Bring Your Own Device (BYOD) Policy

Many Users bring their own personal computing devices (e.g., smartphones, tablets, notebooks, smart watches, and laptops) to conduct University business or otherwise for University

purposes. Users must comply with the University's **Bring Your Own Device (BYOD) POLICY** (Using Your Own Personal Device for University Business) .

Also see: Bring Your Own Device (BYOD) Policy

International Travel

All physical and technical security measures listed in this Handbook should be adhered to when working and traveling within the United States but are especially critical when traveling outside the country.

All Users are responsible for YU-owned devices and YU-owned data on any device that leaves the country, and Users **MUST** report any theft of physical devices or data immediately to infosec@yu.edu.

All Users should check the ITS website - Policy and Procedure page for any specific IT guidelines.

Related Policies in this Handbook:
Information Security & Technology Resources
Physical Security of Technology Resources
Anti-Virus Protection
Remote Access
Work Outside of Yeshiva University's Premises
Also see: Information Security Guidelines for International Travel

Electronic Mail (Email)

Please see the Email Policy on the requirements and proper use of University email accounts, as well as the Mass Email Policy on the requirements and proper use of mass email to disseminate information within and beyond the University.

Related Policies in this Handbook:
Installation and Use of Software
Protection of Confidential Information and Personal Information
Internet Access and Use
Also see: YU email Policy
Also see: YU Mass email policy

University-approved Web/Video Communication and Collaboration

Only YU-licensed applications should be used for communication with both internal and external entities to satisfy security and legal requirements.

Yeshiva University has two approved methods of web conferencing/video calls: Teams and Zoom under YU-owned licenses.

Teams is the primary web conferencing software at YU. Teams should be used for all non-classroom teaching functions, including internal meetings (faculty, departments, etc), meeting with external vendors and all HR related functions, including interviews of candidates.

Zoom was purchased for academic instruction. YU-licensed Zoom accounts should be used for all classroom instruction and academic meetings/purposes. Non-academic use of Zoom requires prior approval by ITS. Exemption requests can be made via the YU Help Desk. No non-YU Zoom accounts should be used for any reason.

Internet Access and Use

Each User is responsible for ensuring that their use of YU's Internet access is consistent with this Handbook, any other applicable University policy, and appropriate business practices. All access to the Internet should use University-supported browsers.

The University may review Internet use, including the amount of time spent on the Internet and sites visited, at any time, for any purpose.

Users should be mindful that Internet sites they visit collect information about visitors. This information will link the User to YU. Users may not visit any site that might in any way cause damage to YU's image or reputation.

Internet sites containing pornography, sexist material, racist material, obscene material, pirated software, or any other inappropriate material may not be accessed without the express authorization of ITS. Further, Internet access shall not be used for any purpose in violation of any law, rule or regulations.

In addition, without the prior approval of ITS, Users may not:

- Change any YU browser security settings;
- Use Technology Resources to deliberately propagate any virus, worm, Trojan horse, trap-door program code or any unauthorized Internet service;
- Download files from the Internet, including web browser add-ins or other such software providing search bars, weather, and screensavers.

Users should be aware that much of the material available on the Internet is copyrighted or trademarked. Other than viewing publicly available material, Users may not use any material found on the Internet in any manner without first establishing that such use would not be in violation of a copyright, trademark or other intellectual property and proprietary rights.

Related Policies in this Handbook:
Using Technology Resources
Installation and Use of Software
Use of Copyrighted Material
Electronic Mail (Email)
See also: Yeshiva University Harassment Policy and Complaint Procedures

Document Retention

All Documents on Technology Resources should be maintained by the User for the duration established by the University's Office of the General Counsel. Immediately upon expiration of the appropriate document retention period, all copies of the Document (physical and electronic) should be destroyed by the User. Information must be destroyed in a manner consistent with the information's level of sensitivity. For example, Users should not place Technology Resources containing Confidential Information or Personal Information in garbage or recycling bins. Instead, Users should contact ITS in compliance with the Technology Resources Disposal policy set forth in this Handbook.

If a User is notified by the University that the University is involved in or subject to an imminent official investigation, litigation, or legal document request, *all Document destruction must cease immediately*. Do not resume Document destruction until specifically instructed by the University's Office of the General Counsel or ITS. Failure to comply with document retention protocols may result in fines, penalties, or sanctions against the User and/or the University.

Related Policies in this Handbook:
Protection of Confidential Information and Personal Information
Technology Resources and Data Disposal
See also: Record Retention Policy.

Compliance and Penalties

All Users must comply with all applicable policies that YU has implemented and may implement from time to time, including this Handbook and all other University policies. Failure to comply with this Handbook or other University policy may result in disciplinary action as more fully described in the University's Employee Handbook, Faculty Handbook and/or other Human Resources or Faculty policies.

Penalties for Violation of Federal Copyright Law

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under Section 106 of the Copyright

Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment and fines.

For more information, please see the website of the U.S. Copyright Office at http://www.copyright.gov, and particularly, its FAQs at http://www.copyright.gov/help/faq.

User Acknowledgment

As part of the annual mandatory Security Awareness training of all administrators, faculty and staff, all Users will be required to acknowledge that they are responsible for reading this Handbook and for knowing and complying with the policies set forth in this Handbook during their employment with Yeshiva University.

COMPLETE AND RETURN THIS PORTION TO THE HUMAN RESOURCES DEPARTMENT WITHIN THREE WEEKS OF EMPLOYMENT AND ONCE PER YEAR AFTER THAT.

I acknowledge that I have read the YU Administration, Faculty and Staff IT Handbook. I understand that I am responsible for knowing and complying with the policies set forth in the Handbook during my employment with Yeshiva University.

I understand that the University has the right to amend, interpret, modify, or withdraw any of the provisions of the Handbook at any time in its sole discretion, with or without notice. Furthermore, I understand that because the University cannot anticipate every issue that may arise during my use of the Technology Resources (as defined in the Handbook), if I have any questions regarding any of the University's policies or procedures, I should consult the University's Information Technology Services Department.

_____

Signature

_____

Printed Name

_____

Title

_____

Date