Policy Name: Electronic Security Policy

Policy Number: 3303

I. Policy Statement

It is Hebrew Union College-Jewish Institute of Religion's (HUC-JIR) policy to create and maintain the security of all forms of HUC-JIR's business information including but not limited to computerized and electronic files and computerized systems, electronic mail (e-mail), network files, workstation and laptop hard drives, and telephone and voicemail systems (hereafter called "HUC-JIR Computerized Systems").

II. Purpose of Policy

An expansion of the policy statement, detailing its obligations and requirements

III. Applicability (Audience)

All employees who have access to files, programs, data, and HUC-JIR intellectual property; whether located on or accessed by a HUC-JIR-owned or personally owned device such as a desktop/laptop computer, smartphone, mobile storage device, flash drive, etc.

IV. Definitions

Provide definitions for any specific terminology in the document.

V. Procedures and Implementation

All employees who work with or have access to sensitive or confidential information must ensure that their computer equipment is inaccessible to others when away from their work area or when traveling. This may include physically securing the equipment/device, closing the program, logging off, locking keyboards, backing up, and proper storage of disks.

Password protection is the individual responsibility of all computer users. Employees are responsible for adherence to HUC-JIR password policies and password change requests when prompted by HUC-JIR Computerized Systems or applications, whether hosted at HUC-JIR facilities or at a host contracted by HUC-JIR. Utilizing another's password or attempting to gain access to other's files without permission may result in appropriate disciplinary action.

Most Recent Revision Effective Date: 6.2022
Initial Adoption Date: 6.2020
Previous Revision Dates: 5.2022

Any attempt by any HUC-JIR employee to intentionally corrupt the network, the system, programs, files, etc., **for any reason** will result in immediate termination and may be grounds for legal action.

All data, text, graphics, and other files created or resident on computers supplied to an employee by HUC-JIR are the property of HUC-JIR. HUC-JIR reserves the right, without prior notice, to access any employee's HUC-JIR-issued computer, files, and/or programs at any time, as well as to change any password as is deemed necessary to ensure proper protection of HUC-JIR information. Monitoring of computer network activity is required for network support and maintenance. Due to this maintenance and support, network connections are monitored and can be logged in order to prevent malware, malicious code, or viruses.

Users should assume that HUC-JIR will record users' access to internet sites, view content of e-mails, record users' access to files and data as well as view the content of any files that are accessed or distributed.

Employees are cautioned that deleting a message or file in no way guarantees that it cannot be retrieved, read, or reproduced in the future. Emails sent to or from the HUC-JIR email system are stored for three years in order to provide legal e-discovery requests when needed.

VI. Enforcement

Employees are responsible for their own actions and management personnel are responsible for ensuring employee compliance with this HUC-JIR policy.

Employees who become aware of a policy violation should immediately report the violation to their supervisor, the Chief Technology Officer and/or the Global Director of Human Resources.

Employees who violate this policy will be subject to disciplinary action, up to and including termination.

VII. Policy Owner, Management and Point of Contact Information

For questions, contact:

E-mail the IT Helpdesk:
helpdesk@huc.edu.

Most Recent Revision Effective Date: 6.2022
Initial Adoption Date: 6.2020
Previous Revision Dates: 5.2022

VIII. Exclusions

None.

IX. Effective Date

June 2022

X. Related HUC-JIR Policies and Documents

3301 Technology Use Policy

3302 Website Accessibility Policy

Identifies related HUC-JIR policies, Code of Regulations (bylaws), and HUC-JIR Board of Governors documents relevant to the policy.

XI. Notification of Policy Changes and Revision History

The College-Institute reserves the right to change this policy at any time. The Electronic Security Policy is posted in the IT section of the HUC website, the Policy Library at 3303 and relevant handbooks.

XII. Appendices, References, and Related Materials

The Appendices provide links to external guidelines, or federal, state, or local laws or regulations relevant to the policy.