Policy Number	711.000
Policy Title	Technology User Onboarding, Transfer, and Offboarding Policy
Responsible Officer	Vice President of Information Technology
Responsible Office	Office of Information Technology
Summary	Policy to establish guidance on technology access, technology equipment, email distribution memberships, data protection, and responsibilities of supervisors and new/departing users at the time of onboarding and offboarding.
Definitions	Data-Any electronic information stored in databases, applications, emails, and/or reports and is sometimes referred to as an electronic record, file, letter, email, or account.
Approving Body	Administrative Council, Academic Council
Approval Date	Admin C 8.7.2024; Aca C 9.13.2024
Last Revision	September 2024
Re-evaluation Date	Fall 2028
Departmental Impact	All users, supervisors, and employees involved in the onboarding and/or offboarding process of CIU and BLS employees and volunteers who require technology access for job functions.

Failure to follow the following policy may result in disciplinary action, including termination of employment.

Policy Statement

This policy ensures the secure, appropriate and timely technology onboarding of new hires, transfer of existing employees, and offboarding of those separating from the organization. This policy establishes governance for technology access, technology equipment, email distribution memberships, data protection, and responsibilities of supervisors and new/departing users at the time of onboarding and offboarding.

Rationale

Technology resources are vital for employees and volunteers who depend on such technology for their job functions. The appropriate notifications to the Office of Information Technology are vital to ensure employees have access to such resources promptly. Additionally, the appropriate notifications to the Office of Information Technology are vital for transfers and departing users to ensure the protection of organizational resources from information security threats and to remain compliant with regulatory data protection and privacy requirements.

Policy Procedures

The following should be adhered to by the organization.

Technology User Onboarding

- New user account requests for employees, adjuncts, student workers or volunteers that require access to technology resources shall be made by the Human Resources and Ben Lippen Administrative offices only. New user accounts will not be created without initiation from these offices.
- New user account requests for temporary contractors must be submitted separately to the Office of Information Technology separately via ticket. A Third-Party Vendor Access Request form must be submitted for contractors.
- The Office of Information Technology shall conduct onboarding/offboarding overview sessions with supervisors to ensure awareness and compliance with the policy.
- Only regular FT/PT University employees shall be added to the University distribution email. Ben Lippen employees, CIU adjuncts, volunteers, student workers, and contractors shall not be included in the University distribution email group. Access to other email distribution groups will be assigned as permitted by data owners per the Data Governance Policy.

- Computers, monitors, and desk phone hardware for new hires must be requested by their respective supervisor by the cutoff period specified in the IT Service Level Agreement (SLA). Failure to do so may result in inadequate hardware not being available on the new hire's start date. Supervisors must request hardware for new employees by submitting the Technology Hardware Request Ticket. Visit the IT Purchases page for information on how to request hardware or software.
- Access to databases must be requested by the employee's respective supervisor. Supervisors should request data access using the Data Access Request Ticket. Access should be requested by their respective supervisor by the cutoff period specified in the IT Service Level Agreement (SLA). Failure to do so may result in insufficient access upon the new hire's start date. Requests for data and database access will require the appropriate approval from the data owners per the Data Governance Policy.
- Supervisors and new employees are responsible for following technology onboarding instructions and completing required onboarding training. Supervisors should contact the IT Help Desk if instructions have not been provided prior to the new employee's start date.
- New hires are responsible for reading the technology handbook, all technology policies on CIU's policy page, IT Service Level Agreement (SLA), and guidelines located on the IT intranet site.

Existing Technology User Transfers to New Departments

- Supervisors of users transferring to their department are responsible for notifying Human Resources of the transfer. The Human Resources office will initiate the IT account transfer request. This request is critical for information security. Transfer requests to the Office of Information Technology will not be performed without initiation by the Human Resources Office.
- The Office of Information Technology shall notify both the new and former supervisor of transferred employees of technology transfers, including hardware, software, and access transfers.
- Unless directed otherwise by the CIO, the Office of Information Technology will own hardware/software used by employees and make final decisions regarding technology reassignments per the Technology Acquisition and Decommissioning Policy.

Technology User Offboarding

- For CIU users that resign or separate from the organization voluntarily, Human Resources should be notified through the normal separation process. The Human Resources Office shall initiate the technology account decommissioning process. Accounts will be deactivated on the separating employee's last workday per Human Resources. Such user accounts will be deleted per the procedures in the Technology Handbook.
- For BLS users that resign or separate from the organization voluntarily, the Ben Lippen Administrative Office will notify the Office of Information Technology to initiate the technology account decommissioning process. Accounts will be deactivated on the separating employee's last workday. Such user accounts will be deleted per the procedures in the Technology Handbook.
- Unless an exception is granted by CIO, requests to keep accounts active beyond the indicated separation date shall not be honored and departing user access will not be kept active beyond the separation date. If the user is performing another position outside of the position they have separated from and must maintain some or all technology access to work, the current supervisor of the user is responsible for notifying the Human Resources Office.
- In the event a user is dismissed involuntarily, the supervisor of the separating employee must immediately notify the Systems Manager, Campus Security, the VP of Information Technology, and Human Resources department. Such immediate separations require time-sensitive action on technology access and equipment and require escalated processing by the Office of Information Technology. To notify the Systems Manager and VP of Information Technology, use the escalation contact information available in the IT Service Level Agreement (SLA).

- Computers, monitors, and desk phones for separating employees must be returned to the Office of Information Technology. Supervisors of separating employees are responsible for collecting the technology equipment and submitting a ticket for IT to pick up the equipment.
- Rarely are devices sold to separating users. In the event separating users have a device that is eligible for resale and are interested in purchasing the wiped device, separating users must follow the Technology Acquisition and Decommissioning Policy to request purchase consideration.
- Access to databases, email, and the network will be deactivated/removed on the date indicated in the User Separation Ticket. For involuntary terminations, all account access is deactivated immediately. Supervisors are responsible for understanding the implications of deactivated access before the separation date.
- Deactivated accounts shall remain deactivated for the duration stated in the Technology Handbook before deletion.
- The Office of Information Technology shall notify the supervisor of the separating employee of offboarding information and responsibilities of the supervisor. Supervisors are responsible for ensuring that the new hire follows the information contained in the notification.
- Separating users are prohibited from copying or transmitting sensitive information from their company-issued technology resources to other locations. Doing so may violate policies such as the Acceptable Use Policy, Data Governance Policy, and related employee offboarding guidelines. Any confidential information authorized during the active work period must be returned to the organization. Likewise, any personal mobile device with sync'd email must be removed from personal devices prior to the separation date.
- Users should not store personal files on the local hard drive of computers or on shared cloud drives. As such, requests to remove or transfer personal files prior to or after separation will not be honored. Intellectual Property approved by the Human Resources department or Deans Offices must be removed before the separation date. The Office of Information Technology will not be responsible for retrieving Intellectual Property lost during the wiping or deactivation of accounts.

Account Freezes and Access Audits

The Office of Information Technology reserves the right to conduct network account audits and freezes at any point in the year and as many times throughout the year to ensure that accounts and access to technology resources are being properly vetted and maintained. Annual account freezes may include adjunct and student worker account requiring annual supervisory confirmation before reactivation. Annual account freezes shall be initiated by the Human Resources Office with the dean's offices for adjuncts and student workers. The Human Resources Office will provide information to the Office of Information Technology regarding account reactivations. Access audits on the main University email distribution list will also be conducted by IT staff in collaboration with the respective data/email distribution list owner(s).

Exceptions

Exceptions to this policy can be submitted to the Office of Information Technology via ticket request. Exception requests shall be reviewed by the Architecture Subcommittee. Given the security and regulatory impact of this policy, exceptions to this policy must be approved by the CIO.

References

Acceptable Use Policy
Data Governance Policy
Technology Hardware and Software Acquisition Policy

Hyperlinks

www.ciu.edu/policy

Revision Table