DEPARTING EMPLOYEES:

Securing Data and Technology Resources

Here are tips from **Information Technology Services** on how supervisors can ensure West Virginia University data and technology resources are properly secured when employees leave the University.

UNIVERSITY EMAIL

- Have departing employees provide a new point of contact to those with whom they regularly interact.
- Set up an away message that automatically provides the new WVU point of contact as soon as possible, and at least two weeks before their end date.
- Add the new contact information to the departing employee's email signature as soon as possible, and at least two weeks before their end date.
- Ensure all important, work-related email content has been shared appropriately with coworkers.
- Ensure all work-related accounts registered to the employee are transferred to another employee.
- If supervisors require access to a departing employee's email account, that request must be submitted no later than 15 days prior to the employee's end date. Approved supervisor access will be limited to 30 days.
- Pursuant to the Electronic Mail Policy, the contents of University-issued email accounts are the property of the University. Departing employees may export contacts from their @mail.wvu.edu account and upload into a personal email account (or @retiree email account if retiring from WVU); however, exporting email content is strictly prohibited.
- Departing employees requesting a University retiree email account should claim it prior to their last day, although they have 365 days to do so.

NETWORK DRIVES

- Departing employees should move any information needed for departmental use from their personal network drive to the department or team's shared network drive.

UNIVERSITY-OWNED EQUIPMENT

- All WVU-owned equipment, including desktops, laptops, or tablets, must be returned to the University.
- Devices should be taken to the appropriate IT support staff to either sanitize and reuse within the University or be scheduled for collection by the University's electronics recycler. IT groups should update their asset inventory accordingly.

REMOVAL OF WVU DATA

- Departing employees MUST delete University data stored on a personally owned laptop, desktop or mobile device. They can download Spirion to find and redact any Sensitive Data that may have accidently been downloaded to a personal device.

SOFTWARE ACCESS

- Access to information systems that use single sign-on will be removed on the employee's end date in MAP; however, ITS also recommends removing all roles granted to the individual within each system to which they have been provided access.
- Supervisors are responsible for ensuring the departing employees have all access and assigned system roles removed from University information systems. Supervisors also should ensure appropriate system(s) access is granted to all existing employees who will be taking over the departing employee's job duties.
- Access to WVU.Encrypted will no longer be provided to the individual after their employment end date. If they require short-term access to the WVU network, they will need to register a new account for WVU.Guest.

CONTACT US:

ITS SERVICE DESK
Phone: 304-293-4444 | 1-877-327-9260
Email: ITShelp@mail.wvu.edu