2021

Technology Service Catalog

OSUIT TECHNOLOGY SERVICES

Table of Contents

Service Desk

Overview

Technology Services (TS) provides OSUIT's centralized technology-support services. The Service Desk is the single point of contact for all requests for technology services. The Technology Service Desk provides a wide variety of services to OSUIT students, faculty, staff, and affiliated stakeholders, supporting the technology necessary to promote increased student-learning outcomes, enhance institutional effectiveness, and improve technology self-efficacy.

Service Desk technologists can, with your permission, remotely access your computer to assist you with problems. The Service Desk technologists will never ask you for your password but will instead request that you enter it when necessary. The Service Desk provides telephone support for as many as 5,000 stakeholders in the use of 1200+ lab machines, 200+ printers, 800+ university-owned employee devices, as well as thousands of personally owned mobile devices. As personally owned devices are not standardized and university-configured and due to the unlimited number of makes, models, and software versions, support for personally owned devices is limited to phone support in connecting to university-provided network resources.

The goal of the Service Desk is to provide timely, accurate, courteous, secure, and best-practice-based first-contact resolution of your service request. It is the goal of the Service Desk technologists to solve your issue before they hang up from your call. Many of the Service Desk staff are ITIL certified to deliver research-based best-practice services. If your request requires a technologist to come to your desk to provide in-person support, a tier two support specialist will be dispatched on a first-come first-served basis, with issues causing campus-wide impact taking a priority over day-to-day individual issues. Phone support is offered at 918-293-4700 from 7:30 a.m. to 4:30 p.m. Monday through Friday. You can enter your request directly into Technology Services ticketing system by sending an email to osuitservicedesk2@okm-kace.osuit.edu. If its after-hours when you realize an issue, email in your request to ensure that it will be at the first of the queue at 7:30am the next business day.

Self-Service Request Portal

TS provides OSUIT's centralized web-based service-management software application that allows TS to coordinate, manage, and track support activities using the ITIL framework. The ITIL framework is a framework of best practices for IT Service Management (ITSM) that aligns IT services with business needs. Self-service ticket requests can be submitted at http://okm-kace.osuit.edu. This portal allows you to monitor the status of your tickets.

Information Technology Security and Compliance

Technology Services, in coordination with OSU System Security and the OneNet Network Operations Center, is responsible for the monitoring of and compliance with information technology policies that apply to the OSUIT campus. Federal, State, and

OSU and A&M System information technology policies and procedures apply to all OSU campuses and stakeholders. These policies can be made more restrictive by OSUIT policies, but may not be relaxed. The State of Oklahoma policies can be found at https://www.ok.gov/cio/documents/InfoSecPPG.pdf. OSUIT technology policies are at https://osuit.edu/policies-procedures/it.php. Adherence to these policies allows the university to protect its data and mitigate security threats, risks, vulnerabilities, and liabilities that threaten the confidentiality, integrity, and availability of data. This helps to ensure that the university can continue to fulfill its mission.

Technology Asset Sanitation

TS provides secure, documented sanitization of removable media from technology equipment. State law and OSU System policy require that all removable media that leave the OSUIT campus outside the custody of OSUIT personnel be properly destroyed and delivered to the State Department of Central Services for secure shredding. This process must be initiated through Fiscal Services. After the persistent storage, usually a hard drive, has been removed and destroyed, the Physical Plant will move the computer equipment to auction storage. After the annual OSUIT auction, the destroyed media is transported to the State of Oklahoma Department of Central Services for documentation of destruction by shredding.

Risk Management

In the process of weighing availability of services, the benefits of 24x7 uptime must be weighed against the costs of the risk mitigation strategies: avoidance, acceptance, transference, and limitation. All technology services require electricity to operate. In the event of a service outage from an electrical utility provider, storm induced power outages, and university physical plant outages due to accidentally cut lines or transmission cabling failure, the resulting loss of electricity will cause all or part of campus technology to fail. Some very simple technology comes right back up when electrical power is restored. Technology such as computers, network devices, and servers, whose systems may be corrupted by the voltage surges, spikes, and drops often resulting from a sudden loss of power, often requires rebooting or reloading to bring the technology back to full functionality.

Avoidance of this risk by using standby generators is the preferred risk mitigation strategy however standby generators capable of maintaining power to the entire university in the event of a power interruption are prohibitively expensive. In the case of short duration power outages under ten minutes the university engages in risk mitigation by using affordable UPS devices on computers, switches, wireless access points and servers. That means university stakeholders who have chosen to use a UPS should not see a degradation of technology services for power outages less than 10 minutes although environmental controls will probably fail until power is restored.

In the event of an outage over 10 minutes in duration, the university chooses to accept the risk, since these outages are infrequent and the cost of avoidance outweighs the inconvenience of loss of information technology availability. Depending on the level of damage caused by the fluctuations in power, most restorations of technology services should occur within four hours of the final restoration of power.

Technology Purchase Consultation and Quotes

All technology purchases and contracts must be approved by TS to ensure connectivity, security, standardization, ease of use, compatibility, and serviceability. TS provides approved quotes to departments wishing to purchase technology equipment. The department can then purchase the equipment by following OSUIT purchasing procedures.

Print Services

TS acts as liaison between our print services vendor and the departments using the multi-function printer devices. These machines can copy, print, fax, scan-to-email, or scan-to-network drives. The Service Desk can, on request, set up access control using a password to allow you to hold print jobs or restrict copying using a password. To improve cost effectiveness, printers can be configured to print in only black and white mode if desired. Toner is automatically shipped to a department by the vendor in advance of complete depletion. These devices print at 45 pages per minute. Using the Auto-Store functionality, they can also perform optical character recognition to create searchable PDF documents. If your department's multi-function printer needs service, please call the Standley Service Desk at 800-522-3725 and give them the five-digit copier number located on the top left side of the body of the copier. If the printer vendor is unable to resolve your problem with a service call, please contact the TS Service Desk at osuitservicedesk2@okm-kace.osuit.edu for escalation of the service request.

Desk-Side Support Services

Overview

TS provides centralized desk-side support services for employee offices and labs. The core of these services involves direct stakeholder support at the location of your technology device and is provided when it is determined by the TS Service Desk that desk-side support is needed. The Service Desk desk-side support team (tier 2) extends the services provided by the Service Desk tier 1 team, who provide first contact resolution. TS services hardware up to four years old purchased through TS with approved service agreements. TS can only offer hardware and software support for university-owned technology devices and software.

Replacement Plan

Technology Services (TS) administers a computer replacement plan program to ensure that employee computers are current enough to run the latest software, operating systems, and security features at speeds that do not negatively affect productivity. The current cycle for replacement of full-time employee primary computers is four years, consistent with the predicable obsolescence described by Moore's Law. This program funds up to the cost of a base-desktop computer, with each department being responsible for any additional cost of customization.

Computer Lab Services

TS installs, updates, and maintains the university's more than 80 computer labs consisting of 1500 devices including printers and switches. OSUIT computer labs provide students, faculty, and staff physical computer access. A computer lab is defined as a set of computers that are identically configured in a single room and virtual accessible equivalents. The labs offer standard suites of software such as Microsoft Office, web browsers, Adobe Creative Cloud, and some labs offer specialized applications such as AutoCAD. Requests for lab software updates must be submitted a minimum of two months in advance. Three months advance is required for upgrades involving new hardware or network wiring changes to allow for the purchasing process. Lab updates are labor intensive and there is a consistent two-month queue year-round. The processing power of new computers more than quadruples over a four-year period, as is described by Moore's Law. Due to the hardware and software incompatibility caused by this predicted obsolescence and the inability to find replacement parts, TS does not support labs with computer hardware older than four years.

Audio-Visual Services

The Technology Service Desk, provides troubleshooting services for department-owned audio-visual equipment and equipment checked out from the Library or the Center for the Advancement of Teaching and Learning (Center). The Library and the Center handle checking out all computer and audio-visual equipment to students and employees respectively. TS supplies a limited number of auction-bound loaner computers for use while an employee's assigned machine is being repaired. Problems with mounted projectors should be directed to the Physical Plant, so they can either un-mount them for replacement, or replace burned out bulbs which will be billed by CVI to departmental accounts.

Sound Reinforcement

TS can provide technical support for high-profile sound reinforcement events planned by the Institutional Event Planning Committee. Please be sure to book your support for a detailed list of equipment, far enough in advance to make sure that TS has available resources. Computers, classroom technology, and sound systems can be checked out by employees from the Center.

Telecommunications

OneNet

OneNet is the Oklahoma State System of Higher Education telecommunications and information network. OneNet is a division of the Oklahoma State Regents for Higher Education. They provide OSUIT with redundant two gigabit per second connections to the Internet as well as 24x7 network monitoring from their network operations center (NOC).

Wired Network

Members of the OSUIT campus community can access the wired network by connecting their university-owned computer to one of the network jacks located in any area which they are authorized to use. All network jacks are 10/100 Mbps capable and are addressed using DHCP. Scarce static IP addresses are reserved for university-owned network infrastructure devices. For network security, availability, confidentiality, and compliance reasons, the use of routers, switches, servers, and wireless access points that are not administered by Technology Services (TS) is not allowed on the university network without prior TS authorization.

Site-to-Site VPN

There are encrypted VPN tunnels setup between the main OSU campus in Stillwater and all branch campuses. All communications between campuses or from off-site are authenticated and securely encrypted over these tunnels.

Off-Campus VPN

OSU requires employees to use secure, encrypted VPN (Virtual Private Network) connections between off-campus devices and OSU's internal network resources on which the university data resources are stored. The OSU System uses the Cisco AnyConnect VPN Client to provide this service. This software can be downloaded by employees at http://osuvpn.okstate.edu. The Cisco Anywhere app is also available on the Apple App Store for use on iOS devices. Other VPN software such as Team Viewer or Splashtop are not allowed to be used to connect to university owned equipment.

Wireless Network

In the academic and administrative buildings on the OSUIT campus and at other participating universities across the world, mobile devices can connect to Eduroam wireless networks depending on your role with the university. Login requires one's university email address and O-Key password. This will allow one to have fast Internet and Intranet access while being mobile. An employee can sponsor a guest for wireless access by calling or emailing the TS Service Desk. Guest account passwords are good for up to seven days.

Your devices generally stay connected to the wireless network unless there is a lack of signal. Mobile devices generally remember credentials until the O-Key password expires or is updated.

You stay connected if you are in range of an access point and seamlessly transfer from access point to access point as you move about campus. This same system is in use across the entire OSU System and higher education using O-Key email address and password.

TS offers landline dial-tone service to departments and schools. All new phones will be IP phones. Calls can be forwarded to another number if desired. Long distance codes may be requested from the Service Desk by a supervisor, in an email. Call logs can be provided on request.

Voicemail

Voicemail is a service that includes receive/save messages, personalized greetings, a personalized password for each employee, and the ability to retrieve messages from on- or off-campus telephones. Voicemail logs can be provided on request.

Call Routing

TS can setup call routes to distribute incoming calls to multiple phones.

Moves, Additions, and Changes to Phone System

TS coordinates phone installation and changes on our Avaya Communications Manager system. Please plan ahead. Changes requiring support from our telephone service vendor require adequate advance notice.

On-Phone Directory

TS can change your directory listing name that appears when someone calls to a digital on-campus phone. Requests for new phones or changes to phone service should be placed with the TS Service Desk. The phone number listed in O-Key is determined by each individual's self-entry in O-Key.

Learning Management System

The OSU System provides the centralized learning management system, known as Canvas. Canvas provides a method for consistent online-course delivery. It can be found at https://canvas.okstate.edu/. This cloud-based resource provides for online-course delivery and support for more than five different campuses within Oklahoma and for fully-online learners across the country thanks to OSUIT's membership in the distance learning State Authorization Reciprocity Agreements organization, SARA. Instructors can receive professional development on instructional design by contacting the Center. The Center provides and supports faculty best practice in instruction and in the use of Canvas. Student scholarship is enhanced by TurnItIn anti-plagiarism software and Respondus Lockdown browser. Non-credit students may use Canvas Catalog in their online studies.

Email

A variety of clients are available to access your OSU employee Outlook 365 mailbox. The Outlook client is available for installation on business workstations. Outlook 365 http://cowboymail.okstate.edu is available from any web browser.
Due to business needs, some individuals may need to delegate e-mail access. TS can assist with these shared calendars, Send on Behalf, or other e-mail settings provided in the email system.

Email Distribution Lists

TS maintains the OSUIT email distribution lists. These lists provide a method for the same email message to be distributed to all members of a defined group of stakeholders. The use of email distribution lists to communicate with OSUIT students, faculty, and

staff will be limited to official notices of university-wide interest or impact. Email distribution lists can either be setup to use Human Resource roles and assignments or can be manually populated by the requestor. Broadcast email may also be used to communicate with the campus community in times of crisis, campus-wide emergencies, and other situations dealing with public safety. Nothing precludes faculty and staff from developing, using, and maintaining their own email lists for legitimate communication needs. Mass mailings in the form of junk mail for non-university business reasons are prohibited. Access to the all student or all employee lists requires a request from a director-level or above supervisor which must be renewed annually.

Microsoft 365

Microsoft 365 allows students mailbox space for storage of Office documents in OneDrive.

Mobile Devices

Mobile devices can be used to connect with Cowboy Mail. A separate document called OSU Email Mobile Device Configuration Settings is available in the IT Resource Center http://it.okstate.edu/rc.

Spam Filtering Services

The OSU System provides a centralized email spam-filtering system named Proof Point. Proof Point offers various spam filtering options that can be set by the employee based on individual preference. Four levels of filtering options are available to OSU employee email account holders: No Spam Filtering, Filter Adult Spam Only, Filter All Spam and Tag and Deliver Spam. For more information, visit http://spamblockerhelp.okstate.edu.

Phone Directory Service

OSUIT Human Resources maintains the university's centralized phone directory service, the OSU Online Directory. Information contained in the OSU Online Directory at http://directory.okstate.edu is business information only and is provided to the public for that purpose. Please remember that the phone number listed is the phone number that you enter in your O-Key account contact information screen. If you enter your home phone number or cell phone number, this is what is displayed to the public on the OSU System websites. It is intended that you publish your work contact information. The university does recognize some situations that an employee may have reason for the information to be removed from the directory and made unavailable to the public. Employees with such a need should provide the Director of Human Services a written request with reasons why this business information should not be available. The Director of Human Resources will review the request and decide whether to allow the information to be removed.

Data Center

Network File Storage

Employees have a minimum of OneDrive, an H: drive, a G: drive, and an I: drive, online file storage that is automatically mounted on university computers. Online file storage

ensures a secure and easily accessible method for file storage and sharing that is not confined to a specific computer. Home (H) drives are the employee's individual storage. Group (G) drives are used to share information within an employee's assigned department. Shared (I) drives are used to share information between departments, committees, or task forces. Network drives are assigned automatically when a person activates his or her O-Key account if they are assigned to a department by Human Resources. TS also provides secure storage that encrypts data at rest and in transit. For assistance, please contact the TS Service Desk. Employee workstations and laptops can also use full-disk encryption if requested. Social security numbers and other personally identifiable information may not be stored on the G:, H:, or I: drives and will be deleted when identified. PII may be stored in secure storage which requires an approved change request with the OSUIT Service Desk.

Enterprise Backup and Restoration Services

TS maintains OSUIT's centralized Enterprise Backup System. These nightly backups enable the university to recover critical data in the event of a disaster or to restore accidentally deleted or corrupted documents that were stored on the network drives.

Disaster Recovery

TS maintains a remote disaster-recovery site for cyber resilience at OneNet in Oklahoma City. In the event of a disaster on the Okmulgee campus, the data center can be restored at OneNet to maintain data operations during the recovery.

Security Cameras

Technology Services (TS) provides server administration and vendor coordination for Avigilon security cameras. Servers and networking must be ordered and administered through TS. To get quote, please contact the Service Desk.

Digital Signage

Technology Services (TS) provides a centralized digital-signage server. Individual departments may connect and post to this system. New signage locations require the department to purchase a display and a minicomputer to mount behind the display. Please contact the Service Desk. Outdoor signage hardware is supported by the Physical Plant. The digital signage content at the 4th Street entrance is cloud-administered by the Office of Marketing and Communications.

Virtual Labs

TS provides virtual labs for students to use from their home or mobile devices. This allows the use of university-owned software on mobile devices using a web interface. Virtual labs can be used at https://desktop.okstate.edu.

Virtual Server Provisioning

TS maintains a high-availability virtual server infrastructure that allows provisioning, restoring, and hosting of virtual servers. The hosted virtual machines' configuration and

content is the responsibility of the owning unit. In the event of a misconfiguration the VM can be quickly restored to the previous days snapshot.

Cloud-Based Collaboration

SharePoint

The OSU System maintains SharePoint, the university's centralized online collaboration system. SharePoint enables groups or individuals to create and configure web sites that meet their specific group-collaboration needs. SharePoint has document libraries, calendaring, lists, and tasks available as well as the capability of building workflows. SharePoint forms with workflow can be used for paperless approval, provisioning, and routing of requests for services. SharePoint allows the use of your O-Key credentials and can integrate into Microsoft Outlook, Teams, and the rest of the Microsoft Office 365 Suite. A link to our SharePoint site along with most of our cloud-based offerings may be found at http://my.okstate.edu.

Video Conferencing/Virtual Meetings

TS can assist with computer-based video conferencing including screen-sharing using web services such as Skype for Business, Teams, and Zoom. If you are joining a meeting using Zoom, Skype, Teams, WebEx, or GoToMeeting, the presenter will send you an email invitation with a meeting code that will allow you to use a web-browser to join the meeting. To avoid delays, participants should allow fifteen to twenty minutes before the meeting to test connections on all sides of the conference. Technology Services can also assist schools and departments with specifications for departmentally owned video conference equipment.

Qualtrics Survey Tool

TS provides a site license for the cloud-based Qualtrics survey tool. Qualtrics enables employees to perform many kinds of data collection and analysis.

O-Key Identity Management

All access to all OSU System resources requires the use of our identity management system, O-Key. O-Key requires proof of identity based on verification of social security number. One of O-Key's core functions is to provide a single, secure user ID and password that can be used to access all university services. After completing your student enrollment or filling out your employment paperwork, you will be eligible for an Orange Key (O-Key) account at http://okey.okstate.edu. By activating your account, you can set up your e-mail address and set up your emergency and directory contact information. Access to secure resources also requires Duo two-factor authentication. Call the Service Desk for more details or go to https://it.okstate.edu/services/multi-factor-authentication/index.html.

O-Key Activation

The ability to activate an individual's profile within the OSU A&M Identity Management System (O-Key) is based solely on that individual maintaining an active association in either the Banner Student Information System or the Banner Human Resources System. This system of record supplies identification and association information to the Identity Management System and assigns specific roles to the individual based on the type of association. These roles provision access to appropriate systems and services.
Currently, the activation process requires the last two characters of the individual's surname, last five digits of their social security number, and the date of birth. The activation wizard will lead you through setting up information such as your username, email address, password, email destination, and various versions of contact information. Activation requires the use of a Personal Identification Number (PIN) sent by email to your Banner alternate email.
The O-Key system is designed to be self-service. Pins required for initial activation are available at the front desk of the Grady Clack Student Success center or by calling the Service Desk. The Grady Clack Front Desk can request an activation reset for forgotten or expired passwords. The only computers on campus that can be used for O-Key activations and resets are the ones at the south side of the Grady Clack Center.

Affiliate Accounts

Individuals who are affiliated with OSU and who can demonstrate a legitimate need to access OSUIT technology resources can apply to the TS Service Desk for an affiliate account. A university department will need to sponsor this access, which will provide all the services associated with an O-Key account. Affiliate accounts must be renewed annually to continue the use of O-Key services. Proof of identity in the form of a social security card, driver's license, and alternate email will be required for processing.

Service Accounts

TS maintains OSUIT's centralized service allocation system via service accounts. Service accounts can be used for many different purposes. You will want to select the appropriate type of service account for your purpose. The different types of accounts are listed below with a brief description of each.

Mail-Enabled Service Accounts

A mail-enabled service account resides in Active Directory and has an Exchange mailbox. This type of account can be used for a departmental email or to receive emails that originate on a Webpage.

Application Service Accounts

An application service account is in Active Directory. It does not have an Exchange mailbox. It is used when you need an application to have access to something else, like LDAP. Please allow a couple of additional days for processing on this type of account because Service Account personnel must submit the account to Service Administration for approval prior to creating the account.

Kiosk Service Accounts

A kiosk service account is in Active Directory. Use this type when you manage public workstations and would like to have them under one service account.

Service Allocation and Access Requests

Access to OSUIT services and resources is based solely on the association an individual maintains with OSU via the Banner Student Information System (SIS) or Human Resources System (HRS). Specific services are provisioned based on the role(s) an individual has been assigned in the Identity Management System, O-Key. The director-level or above supervisor must request access for their employees for additional network drive access and long-distance codes at osuitservicedesk2@okm-kace.osuit.edu.

Emergency Alerts Settings

TS has worked in conjunction with the OSUIT Emergency Management, the Office of Marketing and Communications, and OSU System to develop a mechanism for alerting the campus of weather issues and campus threats. As part of the O-Key activation and at each password reset, contact information is requested to alert an individual in the event of a campus closure or emergency.

Global Groups

Global Groups are available to assist with management of resources. This helps when a person leaves or enters a new home department and needs access to services. Global Groups can be used to permission files or set up email distribution lists.

Authentication Services

The OSU System maintains the university's two centralized directory services (Open LDAP and Active Directory). One of the core functions of OpenLDAP is to support the email spam filtering system. In addition to this functionality, OpenLDAP provides the ability to lookup email addresses, names, departments, and other user information to authenticate applications. The core functions for Active Directory are wireless authentication, workstation management, group management, and group policy management.

CSGold Id System

TS maintains the CSGold and Micros servers that manage ID card provisioning and use. ID cards are issued by Student Services at locations including the Front Desk of the Grady Clack Student Success Center. ID cards can be printed between 15 – 60 minutes after enrollment in Banner. The ID is issued using the name and campus-wide ID (CWID) found in Banner.

Role and Provisioning Management

TS provides provisioning and assignment of appropriate roles and rights for accounts according to established guidelines. Most permissions are assigned automatically based

on the person's roles at the university, however, additional rights may be requested by a director or above supervisor.

Software

Software Installation

Technology Services (TS) provides software installation on university-owned employee computers. Departments can purchase their own specialized licensing and the university provides site licenses for many Microsoft products including Microsoft Office, Qualtrics, and the Adobe Creative Cloud including Photoshop, After Effects, Premiere Pro, InDesign, Flash Professional, Illustrator, Fireworks, Muse, Dreamweaver, Audition, SpeedGrade, Prelude, Lightroom, Flash Builder Premium, InCopy, Acrobat XI Pro, Edge, and Scout. To schedule installation, please contact the Service Desk. New lab software must be requested up three months in advance of desired software usage.

Campus Software Distribution

Stillwater IT manages the free software distribution for the OSU System. Many software packages are available for use on personal computers at http://app.it.okstate.edu/sdc.

Anti-Virus

Active Directory with SCCM enforces automatic installation and updates for anti-malware software. It is designed for Microsoft Windows-based operating systems. This software is necessary to maintain the utility of employee computers as well as to secure the confidentiality, integrity, and availability of data stored on or transmitted by these computers. This software solution must be used on all university-owned Windows based desktop and laptops computers that are joined to the OSU network/domain.

Data Services

Banner Reporting

OSU Stillwater IT maintains the server infrastructure for the Banner Student Information System, Human Resource System, Financial Resources System, SEVIS, Commonline and the Loan Management System for all the OSU campuses and the A&M institutions. Stillwater IT provides software development support, web services support, and production support for these services. TS tier 3 data analysts provide custom Cognos reporting based on data entered and stored in Banner. To request a report, please call the Service Desk (4700) or submit an email ticket to https://osuitservicedesk2@osuit.edu.

ePrint

TS provides services to host documents which were formerly printed and distributed, at http://eprint.okstate.edu. These ePrint documents are generated from the university's administrative systems. A secure authorization model is set up for access to these reports.

Document Imaging

Document imaging is a process through which a document is recorded or scanned electronically, indexed, and stored as a digital image of its original form. Once digitized, it can be routed, archived, and/or retrieved using an installed application or a basic web browser. This service may be implemented as a replacement for traditional, manual filing techniques. Through the document storage and retrieval process, documents are captured by scanning, then indexed and archived for retrieval later. This reduces file space, eliminates errors and misfiling, and improves productivity. Scanned documents can be attached to records in Banner through Grooper scan stations or from the desktop.

New Employee Access to Technology Resources

Technology resources such as computers and peripherals are owned by the employee's department and will be assigned by the new employee's supervisor. All log-on access to technology resources is authenticated through the OSU identity management system, O-Key. A few days after a new employee has been fully processed through our Human Resources department, they will be eligible to activate their O-Key account. O-Key credentials will allow the new employee to log into computer-based devices on campus, network drives, and most other web-based OSU System resources. Multifactor authentication (MFA), DUO, is also required and must be setup when setting up O-Key. For access to computers before the new employee's O-Key is activated, please call the TS Service Desk and they can assign a temporary log-in username and password. The new employee should navigate to http://okey.okstate.edu at least once per day, click the activate O-Key button, and attempt to activate until they are able to successfully create their O-Key account and until they reach the screen informing them that their password will be valid for 120 days. Detailed step-by-step O-Key and DUO activation information is available at http://osuit.edu/okey and https://it.okstate.edu/services/multi-factor-authentication/index.html. All employees who handle student information must successfully complete FERPA training at http://registrar.okstate.edu/FERPA. After the employee has successfully activated their O-Key account and setup MFA, they should log into a computer with their O-Key credentials and use a web browser to navigate to the FERPA training course, read all the material, complete the tutorial at http://registrar.okstate.edu/FERPA. All employees will automatically have an H: drive, a G: drive, and an I: drive assigned based on their roles with the university. Additional access will need to be requested by the employee's director-level-or-above supervisor to the Service Desk at https://osuitservicedesk2@okm-kace.osuit.edu.

Order of Steps for Technology Onboarding:

After the employee has successfully completed HR paperwork the supervisor should:

- request a phone system change from the Service Desk
- request Banner access for the new employee at http://app.it.okstate.edu/access_request/index.php
- assign a computer from departmental resources

Next the employee should:

- sign the Memorandum of Agreement to accept responsibility for the technology assets

- request temporary log in from Service Desk if needed
- attempt to activate O-Key at http://okey.okstate.edu until successful
- discontinue use of the temporary account and start using new O-Key account
- successfully complete FERPA course http://registrar.okstate.edu/FERPA
- upon completion of FERPA tutorial, receive emailed FERPA completion confirmation
- read about the latest-technology services available at http://osuit.edu/ts