IT Practices and Policies

For CWP Network Users

2019

Contents

Back to top

Section 1: General Information Regarding IT Practices and Policies

I. Introduction

Information Technology functions are integral to activities throughout our organization. It is essential that all Capital Workforce Partners (CWP) Network Users use and maintain our IT resources in a way that:

- Protects the organization's investment.
- Ensures the continued effective operation of the systems necessary to meet our business needs.
- Maintains the integrity and security of the information in these systems.
- Utilizes IT resources for business purposes only.

Effective security is a team effort involving the participation and support of every CWP Network User and contractor who interacts with information and/or information systems owned by CWP.

It is the responsibility of all CWP Network Users to understand and comply with these standards in their use of IT systems, data and equipment. These policies also apply to contractors, consultants, temporary staff and other workers at CWP and the American Job Centers (AJCs), including all personnel affiliated with third parties.

II. Roles and Responsibilities

This section provides an overview of the roles and responsibilities of CWP Network Users relating to IT security policies. Specific responsibilities are listed within the individual policy statements.

Note: CWP contracts with an IT services firm for IT support; references to the "IT Helpdesk" pertain to the IT support contractor and its staff assigned to CWP.

A. All CWP Network Users

All CWP Network Users, regardless of their role in the organization, are required to:

- Understand and comply with all IT Practices and Policies.
- Immediately report any security breaches or violations to their unit or site manager, that is, to their CWP manager or their AJC manager.

CWP Network Users must not subvert or try to subvert security measures.

B. Managers and Supervisors

In addition to the above responsibilities, managers and supervisors are required to:

- Ensure that CWP Network Users have a working understanding of the IT Policies and Practices;
- request access for CWP Network Users to secured resources, such as Efforts to Outcomes (ETO), other secured applications, special equipment and remote access;
- take reasonable action to ensure the authorized use and security of such resources;
- report security breaches and violations simultaneously to the IT Helpdesk and CWP Chief Administrative Officer; and
- take appropriate corrective action for violations of security policies.

Back to top

C. Human Resources or Designee: staff on-boarding and exits

In addition to the above responsibilities, a human resources manager or designee, with on-boarding and exit support duties, is required to:

- Request access to network, IT systems and facilities for new hires through the CWP on-boarding process and documentation;
- ensure that all interns, temps, full/part time staff are given this manual and sign an acknowledgement form during the on-boarding process; and
- ensure that the IT Helpdesk and Facilities specialist are notified upon exits of employees so that passwords, accounts and premises access are revoked at exit.

III. Compliance and Monitoring

A. Compliance

Failure to comply with any of the IT Practices and Policies will be addressed by management and/or Human Resources, as with any other violation of CWP policies. Appropriate action will be taken based on the severity of the incident and its impact on our organization.

B. Reporting Security Violations

It is the responsibility of all CWP Network Users to report suspected security violations immediately. Violations are reported to the CWP manager or the AJC site manager, who will in turn report them to the IT Helpdesk and to the CWP Chief Administrative Officer (CAO).

- A security incident is any event, or threat of an event, affecting the normal operation of a CWP managed computer system.
- These include, but are not limited to, electronic intrusions that include networks, servers or workstations; incidents related to catastrophic disasters; and breaches resulting from deception or fraud.

C. Monitoring and Restricting Computer Usage

CWP reserves the right, with or without end-user permission and at any time, to monitor and review any and all information passing through the network. CWP also reserves the right to audit, with or without end-user permission and at any time, all hardware, software and files on any CWP workstation or server.

CWP network users with access to State of Connecticut systems including CTHires, ImpaCT, and the Department of Labor IBM wage reporting system, are subject to State policies.

The State of Connecticut also reserves the right to perform electronic monitoring of any activities involving State computer equipment, databases, and/or other services. The following is an excerpt from the State of Connecticut Electronic Monitoring Notice:

> *"Employees should understand that their activities involving state computer equipment and computer and/or electronic documents, data and communications, including email and Internet usage, are subject to being monitored, recorded and reviewed."*

Back to top

IV. Acceptable Use of Information Technology Resources

A. Ownership of IT Resources

IT resources are provided to CWP Network Users for the purpose of effectively and efficiently conducting CWP business. These resources include:

- Hardware**:** PCs, laptops, tablets, printers, monitors, phones, cell phones, etc.
- Software: All software acquired by or for CWP or developed by or for CWP.
- Data: All data created by employees/contractors/consultants or entered into CWP systems by employees/contractors/consultants.
- Network and Communications Services: Internet, email, voice mail, social media sources, etc.

IT resources are the property of CWP and/or its funders. CWP Network Users are required to use these resources in accordance with the CWP IT Practices and Policies.

B. Acceptable Use of IT Resources

Proper use of resources is described in the policies that follow. CWP Network Users are required to use these resources in a manner that will ensure the security, confidentiality and continued operation of resources, services, data and the CWP network.

C. Unacceptable Use of IT Resources

In addition to the information provided in individual policy statements, general prohibitions follow below. These activities are strictly prohibited. The list is not exhaustive, but it provides a descriptive framework for activity that falls into a category of unacceptable use.

- Engaging in any activity that is illegal under local, state, federal or international law while utilizing CWP-owned resources.
- Using CWP resources to produce work of a commercial nature.
- Violating the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CWP.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and installation of any copyrighted software for which CWP or the end user does not have an active license.
- Exporting software, technical information or encryption technology in violation of international or regional export control laws. The appropriate management should be consulted prior to the export of any material that is in question.
- Using CWP resources to actively engage in procuring or transmitting material that is in violation of state mandated sexual harassment and hostile workplace laws.
- Deliberately bypassing CWP firewalls, anti-virus software or other security protocols.
- Disrupting security, which includes, but is not limited to:
    - Any form of network monitoring with the intent of intercepting data not intended for the user.
    - Port scanning or security scanning.

  - Network sniffing, pinged floods or packet spoofing.
  - Denial of service.
  - Forged routing information.
  - Pushing out spyware, malware and such.
- Making fraudulent offers of products, items or services originating from any CWP account.
- Providing information about, or lists of CWP board members, CWP Network Users or customers to parties outside CWP, except as generally available or as authorized for business purposes by an appropriate Officer.
- Forming contracts. CWP Network Users should be aware that it is possible to form contracts electronically without any paper confirmation from the user. Appropriate authority must be obtained before committing to any contractual obligations (including clicking "I agree" on an online dialog box). The words "subject to contract" should be used on emails where appropriate.
- Connecting personal electronics and cell phones to CWP computers.
- Storing confidential company (CWP, contractor or partner agency) information and client Personally Identifiable Information ("PII") on portable storage devices. Examples include tablets, laptops, cell phones, portable hard drives, USB drives (also known as a flash drives, USB sticks, thumb drives or pen drives), CDs and DVDs. Information security and data retention cannot be on ensured on these devices, and such storage fails against HIPAA and agency requirements.

  Note: CWP IT may support secured, encrypted access to cloud resources for authorized content to authorized persons or teams. Requests may be opened with the IT Helpdesk, and requests are escalated to the CWP Technology Committee for review. CWP policy and US DOL guidance on the protection of Personally Identifiable Information (PII) must be strictly adhered to.

D. Personal Use

Personal use of the Internet, email, social media and other platforms must be limited such that personal use does not affect your ability to complete your job duties.

CWP Network Users are expected to exercise good judgment. Supervisors and managers should provide direction, set expectations and lead by example. Specific directives are:

- Any personal use shall be consistent with the overall principle that the systems are provided for business purposes.
- All use must be in accordance with all applicable laws and policies.
- No personal use shall interfere with a CWP Network User's productivity or performance.

Back to top

Section 2: IT Policy Statements

I. Passwords and Accounts Policy

A strong password policy is essential for maintaining the confidentiality, integrity, and security of the CWP network, systems and data. Three elements are necessary to a successful password policy:

- Password controls exist on all IT systems and computers. Such controls ensure that only authorized CWP Network Users have access to the network or to specific software applications.
- The administration of passwords for providing appropriate access to these systems is in place.
- All CWP Network Users are responsible to properly use and secure their passwords.

A. Password Administration

CWP's IT support contractor is responsible for implementing and administering access controls for all CWP computer systems.

The IT support contractor is also responsible for ensuring that all CWP computers have a password-protected screen saver that will be activated after 15 minutes of inactivity.

B. How to Request Passwords and Accounts

Depending on job responsibilities, an incumbent may have access to and/or passwords for any or all of the resources listed below. In each case, the specified request form must be completed and given to the CWP designee(s) indicated:

Information Technology Confidentiality Agreement

- This form is used to request access to the CWP network and email system; it is submitted to the IT Helpdesk.
- A user account and password are delivered to the new user only after they read, accept and sign the terms in the Agreement.

ETO User Agreement

- This form is used to request access to ETO; it is submitted to CWP's ETO site administrator.

CTHires: Acknowledgement of Receipt of Confidential Information

- This form is used to request access to CTHires from CT DOL; it is submitted to CWP's One-Stop Services Lead.

ImpaCT: Confidentiality and Non-Disclosure Agreement for Contractor Employees

- This form is used to request access to ImpaCT from CT DSS; it is submitted to CWP's One-Stop Services Lead.

C. Password Security

Each CWP Network User is responsible for maintaining the security of his/her computer and all passwords or access codes assigned to him or her. CWP Network Users are prohibited from logging into or accessing any resource for which the CWP Network User is not expressly authorized.

Each CWP Network User is required to:

Back to top

- Be responsible for all computer and electronic transactions made with his or her user ID and password;
- change passwords as directed by each system;
- request a password change immediately if they suspect that the password has been compromised;
- not disable or attempt to bypass the password-protected screen saver;
- not divulge a password to any other person in any form or manner; and
- not log in for another CWP Network User, or other individual, on a network account or a secured online resource.
    - For example, staff are forbidden to log into their assigned accounts and expose company network drives ("H:" or "S:") or client records to a client or guest presenter.

D. General Password Characteristics

This section describes the characteristics of the passwords for some of the resources mentioned above:

- CTHires: Network passwords are administered by the State Department of Labor (DOL). DOL will accept password reset requests only from designated CWP and contractor staff.
- ImpaCT: DSS administers these passwords. Password resets are requested directly from DSS.
- ETO
    - Passwords will be required to be a minimum of 8 characters long.
    - Passwords must contain at least 1 numeric character and at least 1 non-alphanumeric character.
    - Passwords will expire every 180 days.
    - New passwords must not match any of the four previous passwords.
    - Number of unsuccessful log-in attempts before account is locked: 10. After 10 consecutive attempts the account will lock. Locked accounts must be manually unlocked by a site administrator.
- MIP
    - 8 characters (minimum).
    - Password is changed every 90 days.
    - The system does not feature a limit of the number of unsuccessful sign-on attempts before account is disabled.
    - This system can only be accessed by members of an Active Directory security group.
- CWP Network
    - Nine or more characters (strong password complexity is required – see below).
    - System will prompt for a password change every 90 days.
    - Number of unsuccessful sign-on attempts before account is disabled: 5.
    - Restrictions on reusing a previous password are group policy controlled.

- A strong password is comprised of 3 of the following 4 elements listed:
  - Uppercase letters
  - Lowercase letters
  - Numeric
  - Characters such as: !, #, $, %, or whichever others the system allows
- Reset requests for locked network accounts or for forgotten passwords may be made by authorized management. All requests are made with the IT Helpdesk.

II. Virus / Spyware / Malware / Phishing Protection Policy

All CWP Network Users must follow measures to minimize the risk of attacks from viruses, spyware, malware and phishing. These are described in subsection C below.

Constant vigilance against attacks must be maintained as the damage from an attack can be costly to the organization, its partners, contractors, and clients.

CWP has advanced Virus / Spyware / Malware / Phishing protection in place on all computers.

Intentionally bypassing these security systems is prohibited, and violations will be addressed accordingly.

A. CWP Network User Virus / Spyware / Malware Prevention Measures

It is the responsibility of all CWP network users to understand the sources of threats and to use the precautions provided below to prevent outbreaks.

Adherence to these guidelines is crucial to minimize risks:

- Do not disable Antivirus software.
- Do not click on Internet ads.
- Do not open or preview any emails from unknown senders.
- Do not open an unexpected or otherwise suspicious email attachment or link, even from coworkers or business partners.
- Never open an email attachment or link from an unknown or suspicious source.
- Do not download files and/or software from unknown sources.
- Do not surf or access non-business-related websites.
- Do not use your work email address to sign up for non-work-related services.
- If a file you receive contains macros you are unsure about, disable the macros or delete the email.
- Do not install additional Internet browsers. Contact the IT Helpdesk if you have a special requirement.
- Refrain from storing work-related passwords in browsers.
  - *Caution*: Do not sync work passwords stored in Chrome or Firefox with those you store in your personal Chrome or Firefox accounts!

B. Virus Notification

The IT Helpdesk will notify users of credible threats via email or telephone messages. This notification will automatically go to everyone in the organization.

Back to top

C. What to Do If You Suspect You Have a Virus

If you receive a suspicious file or email attachment, do not open it. Contact the IT Helpdesk and inform them that you have received a suspicious file. They will explain how to handle the situation.

If you receive an infected file, notify the person who sent it to you that the file contained a virus or malware.

D. Managing and Tracking Computer Attacks

In the event a virus or other risk is identified, IT Helpdesk will log the potential attack information and problem resolution. The workstation will be quarantined until the IT Helpdesk confirms the intrusion is eliminated, and there are no additional threats.

III. Hardware and Software Policy

A. Procurement

The CWP procurement standard operating procedures apply to all IT resources.

B. Ownership

All hardware and licensed software acquired by or for CWP are the property of CWP.

These resources are to be used for CWP business purposes. All such hardware and software must be used in compliance with applicable licenses, notices, contracts, and agreements.

C. Installation

Hardware and software installation is to be conducted by IT Helpdesk staff only.

D. "Bring Your Own Device" (BYOD)

CWP Network Users are not to bring their own computers or devices to work unless a BYOD Policy has been approved and implemented by CWP management. This does not apply to the use of personal phones for email access.

E. Specialty Software

CWP Network Users needing specialty software should request software via a ticket to the IT Helpdesk.

F. Loaned Equipment

CWP Network Users requiring loaned or temporary equipment for company use, such as hot spots, projectors, and laptops, must submit a formal request for the item to CWP's IT service provider via the standard ticketing procedure. Equipment requests must be submitted one week prior to equipment retrieval and should include the equipment pickup date as well as the return date.

The requested asset(s), if available, will be checked out to the requestor by CWP IT support on the documented date of pickup via CWP's inventory system. Users possessing the loaned equipment are responsible for the return of the equipment on the documented date of return in the submitted request. Time extensions should be requested via an update to the initially submitted equipment ticket.

Back to top

IV. Electronic Communications Policy

Electronic communications include email, voicemail and any form of social media. These resources are provided by CWP for business purposes and all such communications, including attachments, are the property of CWP.

A. Privacy / Confidentiality

Electronic Communications are not private. CWP has access to all electronic communications on its network, which may be monitored at any time.

Users are prohibited from using electronic communications to pass private or confidential information subject to CWP, State and Federal Personally Identifiable Information (PII) policies and regulations.

B. Retention

All email messages sent or received by CWP Network Users are retained subject to the CWP record retention policy.

C. Acceptable Use

All electronic communications must be professional. Please refrain from including any language, tag lines or quotations either in email, voice mail or social media that could be considered political, religious, sexual, or in any way not appropriate to the business of workforce development.

D. Unacceptable Use

Unauthorized Access and Distribution: Accessing another user's email, voicemail or social media is not permitted.

Content: CWP electronic communication resources are not to be used to create, forward or save any communications containing inappropriate language that could be construed as harassing, threatening or discriminatory. Do not include language containing political, religious, sexual, or racial statements.

Security: See Section 2 of this policy manual.

V. Remote Use Policies

These policies address the rules for off-site use of CWP equipment and services. *Remote use is subject to the same IT Practices and Policies as is on-site use*. There are additional considerations due to the portable nature of remote use in non-CWP environments.

- CWP-owned equipment and CWP-provided services are to be used only for CWP business purposes.
- CWP Network Users are expected to take all reasonable precautions to prevent the theft or loss of portable equipment.
- Given that resources are being used in non-CWP environments, special care must be taken to prevent unauthorized access by non-CWP Network Users.

A. Remote Access to the CWP Network

Remote access to the CWP network is provided through Remote Desktop Services (RDS) to only authorized CWP and Partner Staff.

- A computer remotely connected to the CWP network must never be left unattended.

- Remote staff are responsible for all activity on the remote computer and for the security of CWP data and resources.

B. Remote Email Access

Remote email access through Office 365 is available for all CWP network users. No special permissions are needed. Accessing email from home does not constitute permission to work from home.

C. Mobile Device Policy

Mobile devices are issued to CWP Network Users on an approved basis. It is the responsibility of the CWP Network User to protect and secure this equipment.

D. Temporary Equipment Policy

Temporary equipment such as hotspots, projectors, and tablets may be requested via a ticket to the IT Helpdesk. All loaned equipment must be returned by the scheduled due date.

VI. Data Policy

A. Data Ownership

All documents, templates and applications created by a CWP Network User or purchased by the organization are the sole property of CWP.

B. Confidentiality

The information stored and maintained by CWP is considered sensitive and proprietary to CWP unless otherwise identified. CWP Network Users should take the steps necessary to prevent unauthorized access to confidential or proprietary information.

Staff or other users found accessing information without appropriate approval by management and/or in ways considered unauthorized will be subject to disciplinary action.

Non-Disclosure Statements: The CWP Network User Acknowledgement agreement serves as a non-disclosure statement. By signing this statement, you have agreed to protect the confidentiality of all CWP data and client information.

C. Allowable Data

Files saved or copied onto CWP owned workstations, laptops or servers should contain business-related data only.

- Music files, personal pictures or videos are not to be copied onto CWP-owned equipment.

VII. Disaster Recovery / Business Continuity Policy

A. About Disaster Recovery

Disaster Recovery refers to the policies and procedures that must be in place in order to quickly recover from the partial or total loss of computing resources as well as facilities access denial.

There are two components of a Disaster Recovery Plan:

- Ongoing policies and procedures to ensure that recovery is possible; for example, ensuring that adequate backups are in place and that replacement resources are readily obtainable.

- The procedures and detailed steps to follow in the event of a disaster. These must be developed and periodically tested to ensure that they are comprehensive and effective.

Business Continuity refers to the ability of CWP Network Users to continue performing work during a period of time when on-site computing resources or facilities access are unavailable.

- CWP has a separate Disaster Recovery / Business Continuity Plan.

VIII. Equipment Disposition Policy

CWP includes computing devices, defined in 2 CFR 200.20, in addition to other equipment and furnishings in its property records.

Equipment is defined in 2 CFR 200.33 as tangible, nonexpendable personal property having a useful life of more than one year and an acquisition cost of $5,000 or more per unit, including all costs related to the property's final intended use.

A. Property records maintained by CWP shall include specified information:

- Property description
- Serial number or Identification number
- Acquisition date
- Unit Cost Acquisition
- Location of Property
- Disposition date and manner of disposal of property
- Funding source of property identified upon payment
- Assignee's name
- Notes about accessories, ergonomic accommodations and specialized software

Annual physical inventories are conducted by the IT Helpdesk staff and the facilities specialist.

B. Replacement Policy

CWP has adopted an as needed policy on computers / laptops / tablets. These, and all other items will be replaced on the following criteria:

- Broken, damaged, stolen
- The cost to repair the item exceeds 70% of its current estimated value
- Unable to support the necessary software

All purchases must be authorized in the manner described in the CWP Financial Policy Manual. The replacement cycle is dependent on budget availability and may be superseded by the CAO.

C. Disposition of Property

When property is no longer needed by CWP, the IT Helpdesk will submit to the Chief Administrative Officer for signature, written correspondence concerning the disposition of property to the State WIOA Administration or other funding source, if appropriate, or shall submit a memo authorizing the disposition of property by the Chief Administrative Officer.

It is not CWP's policy to refurbish or sell old equipment targeted for disposition, however, in the rare occurrence that old equipment is either retained for another purpose or sold, the applicable funding agency is reimbursed the fair market value of unneeded property retained for use in another program. Any proceeds from the sale or transfer of property are used for the applicable program purpose and recorded against the appropriate fund. Disposition information will be kept on file for auditing purposes.

Back to top

D. Extraordinary Disposition of Property

CWP maintains safeguards to prevent loss, damage or theft of property. Any loss, damage or theft is duly investigated and the results will be documented.

E. Recycling of Property

CWP policy is to recycle retired equipment and consumables whenever practical. CWP attempts to recycle the following items according to the Waste Electrical and Electronic Equipment (WEEE) directives:

- Paper / Cardboard
- Printers / Toner Cartridges / Ink Cartridges
- Faxes
- Computers / Accessories
- Miscellaneous IT Peripherals
- Cell Phones
- Furniture

IX. Capital Workforce and American Job Center Onboarding and Offboarding

A. Capital Workforce Partners User Onboarding

CWP HR will complete a new staff setup/request form and submit it to the IT Helpdesk via the Connectwise Ticketing system at help@novusinsight.com. New user requests must be submitted to the IT Helpdesk at least five business days before the start of employment.

- Request form contents:
    - Full employee name
    - Location of hire and physical location(s)
    - Seating space(s) details, e.g., prior staff names and location descriptions
    - Copier/scanner and printer assignments
    - Distribution group assignments
    - Phone extension assignment
    - Computer equipment and accessory assignments
    - CWP specialty software assignments, e.g., non-routine, licensed software installations for Adobe Pro, Visio, SnagIt, or other
- IT Helpdesk staff will create Active Directory (“company network”) and email accounts and provision permissions for all Active Directory-based systems and copiers. The Helpdesk staff will also configure new-hire computer desktops to documented local requirements.

B. Capital Workforce Partners Offboarding

CWP HR will submit an offboarding request form to the IT Helpdesk via the Connectwise ticketing system at help@novusinsight.com.

- Planned exits:

- For exits involving prior employee notice or a managerial decision, offboarding forms should be submitted to the IT Helpdesk at least two business days in advance.
- Any active dated accounts belonging to ex-employees will remain in place to allow designated managers, specific staff members, etc. access to their information should it be necessary. As designated by management, email forwarding is also in place for any outside vendors or clients that have a need to communicate with CWP.

- Same-day exits:
  - For same day exits, offboarding forms are requested before 1:00 PM to the extent possible.
- Request form contents:
  - Effective date and time of offboarding
  - Alternate offboarding manager name, if any, assigned to complete the exit interview and collect assets
  - Phone status changes, if any, such as call forwarding or voicemail greeting changes
  - Email auto-reply/away message, if any
  - Email forwarding location, if any
  - File/email access by management, if any
- The IT Helpdesk will compile a list of equipment to be collected during an exit interview and notify CWP HR through a Helpdesk ticket response.
- By the requested date and time documented in the ticket, Helpdesk staff will complete the following:
  - Immediately change the Active Directory account/email password.
  - Remove the user account from all currently assigned distribution groups.
  - Convert the user's email box to a shared mailbox in Office 365.
  - Grant managers access permissions requested in the offboarding form.
  - Make requested phone changes including removing the assigned user's name from the extension and setting the phone to "Available".

C. American Job Center User Onboarding

The CWP Facilities Specialist will complete a new staff setup/request form and submit it to the IT Helpdesk via the Connectwise ticketing system at help@novusinsight.com. New user requests must be submitted to the IT Helpdesk at least five business days before the start of employment. AJC managers are requested to inform the CWP Facilities Specialist seven business days before employment start date.

- Request form contents:
  - Full employee name
  - Location of hire and physical location(s)

  - Seating space(s) details, e.g., prior staff names and location description
  - Copier/scanner and printer assignments
  - Distribution group assignments
  - Phone extension assignment
  - Computer equipment and accessory assignments
  - AJC specialty software assignments, e.g., non-routine, licensed software installations for Adobe Pro, Visio, SnagIt, or other
- IT Helpdesk staff will create Active Directory ("company network") and email accounts and provision permissions for all Active Directory-based systems and copiers. The helpdesk will also configure new-hire computer desktops to documented local requirements.

D. American Job Center Offboarding

The CWP Facilities Specialist, or an AJC manager consulting with the Facilities Specialist, will submit an offboarding request form to the IT Helpdesk via the Connectwise ticketing system at help@novusinsight.com.

- Planned exits:
  - For exits involving prior employee notice or a managerial decision, offboarding forms should be submitted to the IT Helpdesk at least two business days in advance. AJC managers are requested to contact the CWP Facilities Manager at least three days in advance.
- Same-day exits:
  - For same day exits, offboarding forms are requested before 1:00 PM, and AJC managers are requested to contact the CWP Facilities Specialist before 11:00 AM, to the extent possible.
- Request form contents:
  - Effective date and time of offboarding
  - Alternate offboarding manager name, if any, assigned to complete the exit interview and collect assets
  - Phone status changes, if any, such as call forwarding or voicemail greeting changes
  - Email auto-reply/away message, if any
  - Email forwarding location, if any
  - File/email access by management, if any
- IT Helpdesk staff will compile a list of equipment to be collected during an exit interview and notify the assigned AJC manager and the CWP Facilities Specialist, via a ticket response.
- By the requested date and time documented in the ticket, IT Helpdesk staff will complete the following:
  - Immediately change the Active Directory account/email password.

- Remove the user account from all currently assigned distribution groups.
- Convert the user's email box to a shared mailbox in Office 365.
- Grant managers access permissions requested in the offboarding form.
- Make requested phone changes including removing the assigned user's name from the extension and setting the phone to "Available".

X. Network Folder Permission Requests

Network folder access permissions and changes can be requested by managers at CWP and the AJC responsible for content in their supervisory areas.

A. Capital Workforce Partners Folder Requests

Network folder permissions and changes can be requested by managers responsible for content in their supervisory areas, while sensitive folders, such as those in Finance and HR, must be approved and verified.

- A manager may submit a support ticket to the IT Helpdesk to request file/folder permissions or changes. The IT Helpdesk will make changes, and the requestor verifies them.
- If the request made is for a sensitive folder, e.g., to the HR or Finance folders, only the HR manager, Controller, CEO and CAO can approve a change, and the IT Helpdesk must verify their approval before making a change.

B. American Job Center Folder Requests

Network folder permissions and changes can be requested by managers responsible for content in their supervisory areas.

- AJC management is responsible for their internal process to select approvers and efficiently communicate only authorized requests and changes to the IT Helpdesk.

XI. CWP Patch Management

All CWP computers are to be automatically patched via the Connectwise management software currently provided by Novus Insight, CWP's IT support provider.

A. Update intervals

- Standard desktops are to be updated via the Connectwise client management software every Thursday evening. Updates will be timed to minimize work disruptions, including for staff in the office after hours between 5:00 – 7:00 PM.
- Organization servers are to be updated during the Novus contracted maintenance window the second weekend of every month.

XII. Forms

Policy Acknowledgment Forms:

- CWP Network User Acknowledgment of IT Practices and Policies (to be signed by all CWP Network Users)
- Acknowledgement of Cell Phone Policy (to be signed by users of CWP-issued cell phones and recipients of CWP cell phone stipends)

Back to top

Request Forms, Sign-out Sheets, Logs:

- Password / Account Request Form
- CWP Disposition Form
- Request for CWP Cell Phone or Use of Personal Phone Stipend

Onboarding and Offboarding Forms:

- Facilities and IT Request Form
- Staff Exit Checklist