Wyoming Judicial Branch

Device Security and Acceptable Use of Information Technology Resource Policy

Policy Approver(s)	Wyoming Judicial Council
Storage Location	wsc-share (Z:) AOC\Common\Policies\Wyoming Judicial Council /Tech Committee
Effective Date	January 1, 2026
Review Period	Annually

I. PURPOSE

The Wyoming Judicial Branch depends on the secure and responsible use of IT resources to uphold judicial processes, safeguard sensitive information, and maintain the public's trust. Misuse or compromise of IT resources could lead to data breaches, legal liabilities, loss of public confidence, and disruptions in critical judicial operations. The security of IT resources is crucial in mitigating risks such as unauthorized access, data breaches, malware, and device loss or theft.

II. SCOPE

This policy applies to all individuals granted access, in whole or part, to the Wyoming Judicial Branch's IT resources, including but not limited to judicial officers such as judges and magistrates, all categories of employees (full-time, part-time, and temporary), contractors and consultants engaged under contract, clerks of district court, and authorized personnel such as court reporters who use IT systems for official proceedings. Additionally, any other individuals authorized by the Wyoming Judicial Branch to access its IT resources are subject to this policy.

III.DEFINITIONS

A. **Acceptable Use:** The use of IT resources in a way that aligns with the branch's objectives, protects data, and complies with policies, legal standards, and ethical guidelines.

B. **Sensitive Information:** Any confidential data that requires protection, including personally identifiable information (PII), court records, financial data, and health-related information.

C. **Branch-Owned or Branch-Issued Devices:** IT equipment provided by the Wyoming Judicial Branch, such as desktops, laptops, tablets, smartphones, and network infrastructure.

D. **Domain Name System (DNS):** A system that translates human-readable domain names (e.g., www.example.com) into IP addresses that computers use to identify each other on the network. The DNS acts as the internet's directory, allowing users to access websites and services without needing to remember numerical IP addresses.

E. **Encryption:** The process of converting data into a coded format to prevent unauthorized access. Encryption is required for all branch-issued devices and personal phones that access Outlook court email.

F. **Personal Devices:** Personal phones or tablets that are authorized to access branch resources, limited to the use of approved M365 apps like Outlook for court email. Personal devices must comply with security requirements, including enrollment in the Mobile Device Management (MDM) system.

G. **Multi-Factor Authentication (MFA):** A security system that requires two or more forms of verification to access branch IT systems, improving access security.

H. **Mobile Device Management (MDM):** A security platform used to manage and secure mobile devices, such as smartphones and iPads, that access branch systems. MDM enforces security policies, manages apps, and enables remote wipe capabilities if a device is lost or stolen.

I. **Patch Management:** The process of applying security updates, bug fixes, and patches to software and operating systems to protect devices from vulnerabilities.

J. **Remote Wipe**: The ability to remotely delete all branch data from a device in the event of loss, theft, or security compromise. Remote wipe capabilities must be enabled for all devices enrolled in the MDM program.

K. **Security Incident:** Any event that poses a threat to the confidentiality, integrity, or availability of the branch’s IT systems or data, including data breaches, malware infections, or unauthorized access.

L. **Unauthorized Access:** Any attempt to gain access to branch systems, devices, or data without proper authorization, including bypassing security controls or using someone else’s credentials.

M. **Unauthorized Software:** Any software not explicitly approved or provided by the IT Division for installation or use on branch-owned devices.

N. **Unauthorized Hardware:** Any hardware device not explicitly approved or provided by the IT Division for connection to or use with branch-owned devices or networks.

O. **Virtual Private Network (VPN):** A secure connection used to encrypt data transmitted between a branch-issued device and the branch’s systems, required for accessing sensitive information when working remotely.

P. IT Resources refer to all technology, systems, and data that are owned, managed, or provided by the Wyoming Judicial Branch to support its operations. These resources include, but are not limited to:

1. **Hardware**: Physical devices such as computers, servers, desktops, laptops, tablets, smartphones, printers, scanners, and external drives.

2. **Software**: All applications, operating systems, programs, and licensed software provided or approved by the Wyoming Judicial Branch for business purposes. This includes office productivity suites, case management software, email clients, and security software.

3. **Networks and Network Equipment**: All networking components, including routers, switches, firewalls, and wireless access points. This also includes any connectivity infrastructure, such as wired and wireless internet, VPN (Virtual Private Network) services, and remote access tools.

4. **Data and Information**: Any data or information stored, processed, or transmitted using branch systems, including case files, court records, employee information, and sensitive or confidential information. This also includes all databases and digital repositories managed by the branch.

5. **Cloud Services and External Systems**: Any third-party services authorized by the Wyoming Judicial Branch for storing, processing, or managing data, such as cloud storage services or cloud-based applications. These services must be approved by the IT Division before use.

6. **Email and Communication Systems**: The branch's email systems, messaging platforms, video conferencing tools, and any other forms of electronic communication used for official business.

7. **Internet and Intranet**: The branch's internet and intranet access and related resources, including the use of browsers, web-based applications, and the secure transmission of data across public or private networks.

8. **Peripheral Devices**: Devices that connect to branch hardware, such as keyboards, mice, monitors, external hard drives, flash drives, and other USB-connected devices.

9. **Mobile Devices**: Smartphones, tablets, or other portable devices provided by the branch or enrolled in the branch's Mobile Device Management (MDM) program.

10. **Security Systems**: The branch’s cybersecurity infrastructure, including firewalls, antivirus software, encryption systems, authentication protocols, and backup systems.

IV. Privacy, Monitoring, and Use Restrictions

A. **Expectation of Privacy:** Users should have no expectation of privacy when using branch-owned IT resources. The Wyoming Judicial Branch may monitor, intercept, and review all activities without prior notice to ensure policy compliance, protect assets, and detect security threats. This applies to all users, regardless of role or access level.

B. **Monitoring:** The branch reserves the right to monitor all IT resource usage to ensure compliance, protect systems, and address security incidents. All users must comply with these protocols.

C. **Use Restrictions:** To ensure the security of the Wyoming Judicial Branch’s IT resources and prevent misuse, the following restrictions are in place for all users.

1. **Access to External Devices:** Users must only connect external storage devices (e.g., USB drives) from trusted sources and must take all necessary precautions to ensure they are free from malware and other cybersecurity threats. Users should request immediate IT review of any unfamiliar or suspect external storage devices.

2. **Access to External Networks:** Branch-issued devices must not connect to unapproved cloud services (e.g., personal Dropbox).

3. **Prohibited Online Services:** Personal web-based services (e.g., Gmail, personal cloud storage) must not be used to transmit or store branch-related data. All official communication and storage must occur through approved branch systems.

4. **Installation of Unauthorized Software:** Users may not install unapproved software or plugins on branch devices or systems. Only software approved by the IT Division or Technology Committee is permitted.

5. **Use of Personal Devices:**

   a. Personal devices can only access M365 apps like Outlook for court email if enrolled in the MDM system. Other use of personal devices to access branch systems or store sensitive information is prohibited.

   b. Personal devices should not be synced with branch systems or applications.

   c. Personal devices are prohibited from connecting to the branch's wifi.

   d. Users must ensure that personal devices enrolled in the MDM program are running the latest available operating system (OS) version and that all M365 apps like Outlook for court email are regularly updated. Failure to apply required updates or maintain the device on the latest available OS may lead to the loss of access to branch email until the device is fully updated and compliant with security policies.

   e. Personal phones used for court email must be secured at all times. Phones must be locked with a strong password, PIN, or biometric authentication and kept in a secure location, especially in public or shared spaces.

6. **Use of Branch Email Accounts:** Branch email accounts must be used exclusively for judicial business. Registering for personal services or using them for non-work-related activities is prohibited.

7. **Data Storage and Transfers:** Branch data must only be stored on approved court systems. Using personal cloud services or unapproved platforms for judicial data is forbidden.

8. **Misuse of Resources for Personal Gain:** IT resources must not be used for personal gain, side businesses, or non-branch-related activities, including commercial, political, or social purposes.

D. **DNS Content Filtering:** To safeguard the Wyoming Judicial Branch's network from malicious sites, phishing, and unauthorized content, DNS content filtering will be enforced across all branch networks and devices. Any attempt to bypass these filters, such as using unauthorized VPNs, proxies, or alternate DNS settings, is strictly prohibited. The DNS filtering system will automatically block or restrict access to websites and services, including but not limited to those that:

1. Pose known security risks, such as phishing, malware, or ransomware distribution sites.

2. Are classified as non-business related, such as gaming, social media, audio and video streaming, or unauthorized file-sharing platforms.

3. Are known to host objectionable or illegal content.

E. Stale Device: Devices issued by the Branch or personal devices used to access Branch systems that are inactive for more than 30 consecutive days will be classified as stale and automatically blocked from network access.

1. Automatic Block: Stale devices will be blocked from the network until reauthorized by IT.

2. Reactivation: Users must contact IT to request reauthorization. Devices will require a security check and updates before regaining access.

V. DEVICE SECURITY REQUIREMENTS

To protect Wyoming Judicial Branch IT resources, all branch issued and personal devices must adhere to strict security configurations, management policies, and acceptable use standards.

A. Security Configuration & Management

1. Mandatory Security Features

a. All devices (desktops, laptops, iPads, and phones) must be configured with encryption, endpoint protection, DNS filtering, patch management, and firewall settings.

2. Device Management & Updates

a. Branch-issued devices are centrally managed by the IT Division to enforce security policies, control software, and apply automatic updates.

b. Users must allow all system updates and patches to complete as scheduled. Interfering with update processes is not permitted.

3. Approved Software & Apps

a. Only IT-approved software and applications may be installed on branch-issued devices. Unauthorized software is prohibited.

b. iPads will have app stores removed, and only approved business-related applications will be installed.

c. Additional software requests must be submitted in accordance with the exemption process outlined in the Hardware and Software Policy.

B. Device Usage & Access Controls

1. Work-Related Use

a. Desktops are for in-office use only and must be secured when not in use.

b. Laptops may be used on-site or remotely but must always be secured.

c. Branch-issued phones are intended for work-related communication. Incidental personal use (calls, texts) is allowed if it does not interfere with security or work duties.

VI. ACCEPTABLE USE

A. **General Guidelines:** Users must use IT resources responsibly, securely, and ethically to support the mission of the Wyoming Judicial Branch and maintain the integrity of its operations. This includes:

1. Conducting all online and digital activities with professionalism and integrity.

2. Refraining from any use of IT resources for personal gain, unauthorized activities, or actions that could negatively impact the reputation of the branch or its personnel.

3. Ensuring ongoing compliance by regularly reviewing and understanding the latest policies and updates from the IT Division or the Technology Committee.

B. **Protection of Information:** Users are responsible for safeguarding sensitive and confidential information. This includes:

1. Protecting data from *unauthorized* access, modification, disclosure, or destruction, regardless of whether the data is in transit, at rest, or in use.

2. Utilizing encryption, strong passwords, and multi-factor authentication (MFA). Branch-issued desktops must have encryption, endpoint protection, DNS filtering, patch management, and firewall settings. Altering or disabling these is prohibited.

C. **Responsibility for Equipment:** Users are expected to properly maintain and safeguard branch-issued IT devices, ensuring they are used for their intended business purposes. This includes:

1. Handling branch-issued devices (e.g., laptops, tablets, mobile phones) with care and ensuring that they always remain secure, particularly during travel or when working remotely.

2. Reporting any lost, stolen, or damaged devices immediately to the IT Division. This includes personal devices that are used to access court data.

3. Ensuring that devices are returned in good working condition when they are no longer required or upon termination of employment or contract.

4. Ensuring that all software updates, security patches, and maintenance schedules are followed to keep the device secure and operational.

5. Refraining from placing stickers, labels, or any other unauthorized markings on branch-owned IT devices to maintain a professional appearance and prevent potential damage to the equipment.

D. **Accountability and Reporting:** Users are personally accountable for any actions taken under their assigned credentials. Any suspicious activity, security incidents, or violations of this policy must be reported immediately to the IT Division.

VII. UNACCEPTABLE USE

A. **Prohibited Activities:** Users are strictly prohibited from engaging in the following activities:

1. **Unauthorized Access:** Attempting to gain unauthorized access to systems, networks, or data, whether within or outside the branch.

2. **Malicious Actions:** Introducing or propagating malicious software (e.g., viruses, ransomware) into branch systems.

3. **Inappropriate Content:** Accessing, storing, or distributing content that is offensive, illegal, or discriminatory, including pornography, hate speech, or harassment.

4. **Circumventing Security Controls:** Tampering with or bypassing security controls such as firewalls, anti-virus software, or access controls.

5. **Accessing Court Systems for Personal Use:** Accessing court systems, databases, or platforms for personal reasons is strictly forbidden. This includes:

   a. Using court systems to settle personal disputes or gather information for non-work-related purposes.

   b. Accessing confidential or sealed case information without authorization.

6. **Unauthorized Access to Case Information:** Accessing, modifying, or sharing case-related information without proper authorization is prohibited, regardless of its confidentiality. Users may only access information necessary for their job and must not use privileged access for personal interest. This includes:

   a. Accessing case files out of curiosity or for personal research.

   b. Sharing case information with unauthorized parties, including friends, family, or the media.

   c. Using privileged access to obtain information on cases that are unrelated to the user's professional responsibilities.

7. **Prohibited Use of Personal Devices on Private Wi-Fi Networks**: Personal devices are prohibited from connecting to the Wyoming Judicial Branch's private Wi-Fi networks. Only branch-issued and IT-approved devices are authorized for business use on the private network.

8. **Catch-All Provision**: Any hardware, software or activity not explicitly mentioned but determined by the IT Division to pose a security risk or threaten IT resources is prohibited. The IT Division reserves the right to implement further restrictions or take necessary actions to protect branch networks, devices, systems and data.

VIII. OCCASIONAL AND INCIDENTAL PERSONAL USE

While branch IT resources are primarily for work-related tasks supporting the Wyoming Judicial Branch's mission, occasional incidental personal use is allowed under strict conditions. Personal use must not hinder job performance or compromise system security, performance, or availability. The following guidelines apply:

A. **Limited Duration:** Personal use must always comply with branch security policies and must never compromise the integrity of the branch's IT infrastructure.

B. **No Use of Bandwidth-Heavy Services:** Personal activities that consume excessive bandwidth are prohibited, as they can impact branch operations.

   1. **No Video Streaming:** Personal use of video streaming services like Netflix or Hulu is not allowed on branch networks due to bandwidth concerns.

   2. **No Music Streaming**: Streaming music from services like Spotify or Apple Music is also prohibited. Users should use personal devices and data plans for entertainment during breaks.

3. **No Large Downloads:** Downloading large personal files (e.g., software, games, movies) on branch systems is forbidden to avoid network performance issues.

C. **Data Privacy and Monitoring:** Users should be aware that all activities on branch-owned IT systems or devices, including personal use, are subject to monitoring.

1. Personal activities may be logged and reviewed by the IT Division to ensure policy compliance.

IX. REMOTE WORK AND DEVICE SECURITY

A. VPN and Secure Access

1. **VPN for Branch-Issued Devices:** All remote access to branch systems from branch-issued devices must occur via the branch's VPN, ensuring encrypted data transmission.

   a. **Mandatory VPN Use**: Branch-issued devices must always use the VPN when accessing internal systems or sensitive information, such as case management systems and file servers.

   b. **Public Wi-Fi Restrictions**: Users must not use public or unsecured Wi-Fi to access branch systems without connecting through the VPN. The VPN must be active before accessing any branch resources.

2. **Multi-Factor Authentication (MFA) for Remote Access:** MFA is required for remote access to branch systems to ensure only authorized users can gain access.

   a. **Mandatory for All Remote Access**: MFA is required for accessing systems such as email, case management, and file servers. This adds a second layer of protection even if a password is compromised.

   b. **User Responsibility**: Users must properly complete MFA during each session. Any issues with MFA should be reported to the IT Division immediately to prevent unauthorized access.

3. **Secure Network Connections:** All users working remotely must ensure they connect from a secure, trusted network.

   a. **Home Network Security**: Users must secure their home Wi-Fi with strong passwords and encryption (e.g., WPA2 or WPA3) to prevent unauthorized access.

   b. **Personal Hotspots**: If home networks are unavailable, users should use a personal mobile hotspot instead of public Wi-Fi. The VPN must be used in all cases.

X. COURT REPORTER EQUIPMENT AND VLAN ACCESS

Court reporters use personal equipment for official duties and must follow strict security measures to ensure the integrity of the Wyoming Judicial Branch's IT systems. They are limited to accessing branch applications through a dedicated Court Reporter VLAN via the Court's VPN and are prohibited from accessing the main Court's WAN.

A. Court Reporter Equipment Requirements:

1. **Secure Configuration:** Court reporters' devices must comply with branch security standards, including up-to-date operating systems, antivirus software, and system patches.

2. **Access Restrictions:** Only the dedicated Court Reporter VLAN may be accessed via the Court's VPN; access to the main WAN or other branch networks is prohibited.

3. **Network Segregation:** The Court Reporter VLAN is isolated from the main WAN. Attempts to bridge or connect devices between the VLAN and WAN are forbidden and may lead to disciplinary action.

B. **Security Monitoring and Compliance:** Court reporter equipment will be subject to periodic security audits and monitoring while connected to the Court Reporter VLAN and VPN to ensure compliance with the branch's security policies. Unauthorized devices, improper configurations, or any attempt to bypass VLAN or VPN restrictions will result in immediate revocation of access and potential disciplinary measures.

C. **Incident Reporting:** Court reporters must immediately report any security incidents, including lost or stolen equipment, unauthorized access attempts, or suspected malware infections, to the IT Division. Prompt reporting ensures that the necessary steps can be taken to protect the branch's systems and data.

D. **Network and Data Use Limitations:** Court reporters are responsible for ensuring that their equipment is used strictly for official court reporting purposes. Personal use of devices while connected to the Court Reporter VLAN or VPN is prohibited. Court reporters must not use unapproved software or services that could pose a risk to the network or branch systems.

XI. CLERKS OF DISTRICT COURT EQUIPMENT AND VPN ACCESS

Clerks of District Court, while not branch employees, are granted access to certain Wyoming Judicial Branch resources for official duties. To ensure security, they must follow these requirements when accessing resources via the Court's VPN.

A. **Clerks of District Court Equipment Requirements:**

1. **Secure Configuration:** Devices must comply with branch security standards, including up-to-date antivirus software and required system patches.

2. **VPN Access Only:** Access is limited to the Court's VPN on county-issued computers. Direct access to the Court's WAN or other internal networks is prohibited.

3. **Authentication:** Clerks must use strong passwords and, when required, multi-factor authentication (MFA) to access court systems.

B. **Security Monitoring and Compliance:** The devices used by Clerks of District Court will be subject to periodic monitoring and security audits while connected to the Court's VPN. Unauthorized devices, improper security configurations, or attempts to bypass the VPN will result in immediate revocation of access to branch resources.

C. **Incident Reporting:** Clerks of District Court must promptly report any security incidents, such as lost or stolen equipment, unauthorized access attempts, or potential malware infections, to the branch's IT Division. Prompt reporting will ensure swift action to protect branch systems and prevent further risk.

XII. OTHER USERS

Other Users granted access to Wyoming Judicial Branch resources for official duties must adhere to the following security requirements when accessing branch resources via the Court's VPN:

A. Equipment Requirements:

1. Secure Configuration: All devices must comply with branch security standards, including up-to-date antivirus software and required operating system patches.

2. VPN Access Only: Access to branch resources is only permitted via the Court's VPN. Direct access to the Court's WAN or internal networks is prohibited.

3. Authentication: Users must use strong passwords and, where required, multi-factor authentication (MFA) to access court systems via the VPN.

B. Security Monitoring and Compliance: Devices will be subject to periodic monitoring and security audits while connected to the VPN. Unauthorized devices, improper configurations, or attempts to bypass the VPN will result in revoked access.

C. Incident Reporting: Users must promptly report any security incidents, such as lost/stolen equipment, unauthorized access, or malware infections, to the IT Division to protect branch systems and prevent further risks.

XIII. INDIVIDUAL ACCOUNTABILITY

Every user is personally responsible for all actions carried out under their user ID or login credentials. The following measures must be adhered to:

A. Password Security: Users must create strong, unique passwords per the branch's Identification and *Authentication Policy*. Passwords are critical to protecting against unauthorized access and must be handled with care.

1. Writing down passwords or storing them in unapproved, unencrypted files is prohibited. Approved password managers are encouraged.

B. Locking Workstations: Users must lock their computers or mobile devices whenever stepping away, even briefly, to prevent unauthorized access, especially in shared spaces.

1. **Automatic Locking:** Devices are set to lock after 15 minutes of inactivity, and these settings must not be changed.

2. **Manual Locking:** Users should manually lock devices when leaving their workstations, whether in the office or remotely.

3. **Remote Device Locking:** Branch-issued devices must be locked when not in use, especially in public or shared environments like airports or cafes.

C. Credential Sharing: Sharing login credentials or authentication tokens is strictly prohibited. Users are accountable for all actions under their account, and sharing undermines the security of branch systems.

1. **No Shared Access:** Credentials, including passwords, security tokens, or MFA codes, must not be shared with anyone, even in urgent situations. Users should request proper access delegation from the IT Division if needed.

2. **Unique User Access:** Users must access systems using their unique credentials. Shared or group accounts are prohibited unless specifically authorized by the IT Division for technical purposes.

3. **MFA Tokens:** Users required to use MFA must keep their tokens or devices secure. Lost or compromised tokens must be reported immediately to the IT Division.

D. **Incident Reporting:** All users have an obligation to promptly report any suspicious activities, unauthorized access attempts, or potential security incidents to the IT Division as outlined in the *Incident Response Policy*.

E. **Device Security On-Site and Off-Site:** Users are responsible for securing all branch-issued devices, both when working on-site at branch facilities and during off-site use, including while traveling or working remotely. Users must follow all branch security guidelines to prevent loss, theft, or unauthorized access to devices.

XIV. ENFORCEMENT AND COMPLIANCE

Non-compliance with this policy may result in disciplinary actions, including but not limited to revocation of access privileges, termination of employment, or legal action. Regular reviews will ensure ongoing compliance.

XV. POLICY EXCEPTIONS

Exceptions to this policy may be granted for specific operational or business needs. Exceptions require a formal request submitted through the Help Desk and evaluated by the Technology Committee. Each request will be evaluated to ensure it doesn't compromise system security or integrity using the following guidelines:

A. Specific Policy or Requirement: Clearly identify the specific policy or requirement for which an exception is being requested. This ensures that the request is properly evaluated in the context of the relevant security controls.

B. Justification for the Exception: Provide a detailed justification for the exception. This should include the business need, operational requirement, or any unique circumstance that makes compliance with the current policy impractical or counterproductive.

C. Proposed Duration of the Exception: Specify whether the requested exception is temporary or permanent. If temporary, indicate the anticipated duration, and if permanent, explain why the exception must be long-term.

Approved By:

Lynne Boomgaarden   8/8/2025

Lynne Boomgaarden, Chief Justice
Chair, Wyoming Judicial Council

Date