

[Compliance] University Policy Updates

From Ccr_all_employees <ccr_all_employees-bounces@lists.wsu.edu>
on behalf of
All employees <ccr_all_employees@lists.wsu.edu>
Date Thu 7/23/2026 12:00 PM
To All employees <ccr_all_employees@lists.wsu.edu>

1 attachment (473 bytes)
ATT00001.txt;



Policies, Records, and Forms

WASHINGTON STATE UNIVERSITY

Policy Changes

Below is a table summarizing new administrative policies, WAC rules, and revisions approved and published January 1, 2026, through the present date.

For a complete list of published policy revisions, please see the [Past Policy Revisions page](#) on the Policies, Records, and Forms (PRF) website. For current revisions and new policies in progress, please see the [Policies Currently Under Review page](#) on the PRF website. A comprehensive, searchable list of current University-wide policies is available on the [Policies Homepage](#).

All University employees are responsible for being aware of and complying with University policies and rules that apply to their employment and other WSU-related activities.

Table 1: Summary of Policy Changes

Policy Name	Policy Number (linked)	Summary of Changes
Parking and Traffic Regulations for WSU Tri-Cities	WAC 504-13	This revision: • Updates language and permit information for individuals with disabilities; • Removes outdated parking permit and payment options; • Removes wheel lock eligibility list and use; • Simplifies enforcement authority of WSUTC and times of enforcement; • Updates qualifications and outcomes of impounding vehicles; • Expands vehicles to include other forms of “micro mobility devices”; and • Updates list of definitions to match the chapter.
Standards of Conduct for Students	WAC 504-26	This revision: • Broadens the list of acceptable academic and appeals hearing board members; • Updates requirements and processes for hearings and appeals boards; • Includes the process for conduct officer hearings; • Specifies parties and parties’ rights in hearings; • Clarifies processes for full adjudications and brief adjudications;

		- Aligns harassment and hazing definitions, prohibitions, and resources with University and state requirements; and - Expands good faith exemptions.
Policy on Policies	UPPM 10.38	This revision: - Adds Section 5.3 Appendix and Form Revisions, which clarifies revision processes to these components when not included as part of a full policy revision; and - Updates links to reflect current webpages.
Facility Naming Policy	UPPM 20.36	This revision: - Adds EVPFO authority to refer projects to Facility Names Committee; - Includes "gifts in place," such as statues and memorial structures, as minor facilities; - Emphasizes that honorific naming is only permitted in rare and exceptional circumstances; and - Clarifies WSU's right to deny naming requests.
Processing Non-Grant Receivables in myWSU	UPPM 30.57	This revision: - Changes the name of the policy from "Student Financial System" to "Processing Non-Grant Receivables in myWSU"; - Creates a fillable PDF of the WSU Invoice for departmental use; - States the purpose and applicability of the policy; - Updates invoice completion, numbering, and distribution requirements; and - Adds information on billing and aging reports through the Bursar's Office.
Payment Card Data Security Compliance	UPPM 30.61	This revision: - Adds responsibilities regarding merchant and terminal accounts; - Updates website and third-party processing security requirements; - Simplifies process for PCI DSS assessments; and - Updates links and titles throughout.
Direct Deposit of Excess Financial Aid Funds	UPPM 30.98	This revision: - Clarifies the purpose of the policy; - Adds information on physical checks sent to out-of-date mailing addresses; - Updates direct deposit enrollment information to reflect current TouchNet procedures and requirements; and - Updates timeline of disbursement.
Proposal Processing and Development	UPPM 40.02	This revision: - Updates the proposal approval process; - Adds time requirements for completing the eRex form; - Clarifies waiver requirements; - Clarifies executive signatures requirements; and - Updates relevant position and department titles.
Departmental Recognition Awards	UPPM 55.56	This revision: - Adds HRS as an additional policy owner; - Changes the name of the policy from "Cash Awards to WSU Employees" to "Departmental Recognition Awards"; - Clarifies that the policy applies solely to departmental and unit recognition awards under RCW 41.60.150 and does not apply to centrally funded awards; - Clarifies that the \$200 limit for these awards applies regardless of the source of WSU funds; and - Specifies the time required for physical checks to be processed.

Administrative Professional Salary Determination and Adjustment	UPPM 60.12	This revision: • Updates the conditions when a stipend is appropriate; • Adds a section outlining the need and requirements for temporary salary increases; • Adds “extraordinary merit” as a reason for an out-of-cycle salary adjustment; • Updates the HRS process for reviewing an employee-requested position review; • Adds a section outlining the requirements and process for a management-requested position review; and • Updates formatting and links.
Partner and Spouse Accommodation	UPPM 60.15	This revision: • Changes proposal approval from the Vice Provost for Faculty Development and Recognition to the Office of the Provost generally; • Includes HRS in the departmental proposal development process; • Acknowledges “dual career” terminology; • Updates the criteria for position support after the end of temporary employment; • Adjusts formatting to match current policy template; and • Updates links to resources throughout.
Recruitment and Selection of Classified Positions	UPPM 60.18	This revision: • Removes references to protected and underrepresented classes when discussing equal opportunity employment; • Includes Recruiter and HRS in steps throughout the recruitment process; • Updates steps for changing an applicant’s status during the interview process; • Simplifies exceptional circumstances for exceptions to open recruitment; • States requirements for direct appointments not handled through Workday; and • Updates links to resources throughout.
Reasonable Accommodation of Employees	UPPM 60.21	This revision: • Changes the policy name from “Reasonable Accommodation” to “Reasonable Accommodation of Employees”; • Clarifies language around job functions; • Adds functions of an employee type, such as faculty modality requirements, to evaluation considerations for accommodation requests; • Provides PFML references within Section 4.6.e Disability Separation; • Includes all eligible individuals in Section 4.0 Requirements; • Corrects citations, grammar, and links; and • Updates formatting to match current policy template.
Probationary and Trial Service Periods for Civil Service Employees	UPPM 60.31	This revision: • Adds “breaks in service” to circumstances requiring probationary periods; and • Updates position titles for accuracy.
Faculty and Administrative Professional Personnel Leave	UPPM 60.56	This revision: • Defines “family member” in accordance with WAC language; • Includes specific timeframes for LWOP, FML, and Military Leave use; • Updates requirements for use of leave based on current WAC language; • Clarifies prorated accrual for all types of leave; • Clarifies eligibility for concurrent use of disability leave and FML; • Includes “maintaining benefits eligibility” in all uses of extended leave; and • Adds “hate crime” to Section 24.0 and expands the applicability and requirements.

Civil Service Employee Leave	UPPM 60.57	This revision: • Updates requirements for confirming time worked; • Includes nonpermanent employees; • Clarifies prorated accrual for all types of leave; • Clarifies recourse for leave accumulation exceeding 280 hours; • Updates process for continuing benefits in cases of extended LWOP or disability leave; and • Adds “hate crime” to Section 24.0 and expands the applicability and requirements.
Training and Development	UPPM 60.71	This revision: • Incorporates and updates information on release time for training (section 3.0) from UPPM 60.72 Release Time for Training, which will be retired; • Updates training and development expectations; • Clarifies documentation requirements for training; and • Updates links to HRS resources and contact information.
Minor Construction, Renovation, Remodeling, and Demolition	UPPM 80.56	This revision: • Clarifies fees and bid thresholds for public works projects; • Clarifies requirements for proposals and initial review of projects; • Updates process and links for submitting project requests and relevant forms; and • Adds more specific language to requirements and limitations throughout.
Account, Identity, and Authentication Management	UPPM 87.03	Policy overview: Appropriate criteria and robust controls regarding account, identity, and authentication management are critical to ensure the confidentiality, privacy, integrity, and availability of institutional systems and data. This policy sets forth the roles, responsibilities, and requirements to ensure WSU’s compliance with applicable standards, thereby advancing WSU’s academic, research, and administrative missions.
Access Control and Authorization	UPPM 87.05	Policy overview: Robust access control and authorization serve as critical safeguards for WSU’s information systems by ensuring that only authorized individuals can access specific data, applications, devices, and systems. This policy reduces the risk of unauthorized access to information systems and institutional data by establishing criteria related to access control and authorization, including specific requirements for moderate- and high-impact systems.
E-Mail Use and Security	UPPM 87.07	Policy overview: WSU and each user of WSU email and systems have an obligation to ensure the security, integrity, and accessibility of records sent or received by email, as well as appropriate use of WSU email systems. To fulfill these obligations, this policy: • Clarifies the duties of all persons utilizing WSU email accounts, with additional duties for those persons conducting official WSU business; • Sets forth requirements to reduce the risk of unauthorized access or disclosure of WSU institutional data; and • Helps to ensure that public records are retained and accessible as required by law.
Electronic Device (Endpoint) Security	UPPM 87.10	Policy overview: The security of endpoints, including but not limited to smartphones, tablets, and computers, is critical to protect institutional data and prevent unauthorized access and other security threats to WSU systems. This policy sets forth requirements for the use of WSU-owned or employee-owned endpoints for the purpose of creating, storing, transmitting, and protecting institutional data.

Network Security	UPPM 87.12	Policy overview: Safeguarding the security of WSU's network infrastructure protects WSU data, ensures the integrity of WSU's IT environment, and supports WSU's critical academic, research, and business functions. This policy sets forth the roles, responsibilities, and requirements that relate to the security of WSU's network.
Information Security Planning	UPPM 87.15	Policy overview: Comprehensive information system security planning safeguards WSU data, systems, and information technology resources from evolving threats. This policy sets forth roles, responsibilities, and requirements to ensure robust and thorough system security planning, thereby supporting and advancing the University's academic, research, and administrative missions.
Vulnerability Management	UPPM 87.17	Policy overview: Establishing uniform requirements for identifying, assessing, and remediating vulnerabilities within WSU's information systems helps reduce security risks and protects institutional data. This policy supports WSU's overall information assurance program by defining expectations for vulnerability scanning, reporting, and coordinated remediation efforts across the University.
Security Assessment and Authorization	UPPM 87.20	Policy overview: Evaluating and authorizing information systems through the use of structured, risk based security assessments helps ensure the security of WSU systems and protects WSU systems and data. This policy establishes roles, responsibilities, and requirements for security assessments and reports, testing, monitoring, and security authorization and reauthorization across the University.
Security Awareness and Training	UPPM 87.21	Policy overview: To support the integrity of WSU's technology resources, all WSU personnel must have the knowledge and skills to identify, prevent, and respond to potential security risks. Users handling sensitive data are required to have additional training appropriate to their role. The purpose of this policy is to ensure that all users of WSU email, applications, and other computing resources receive adequate training to understand and adhere to best practices in information security.
Control Exception	UPPM 87.23	Policy overview: The policies in Chapter 87: Information Technology and Security set forth requirements intended to protect WSU's technology resources and institutional data. However, WSU recognizes there may be exceptional circumstances in which adherence to established policies and/or standards could inadvertently hinder critical academic, scholarly, outreach, or operational activities. This policy sets forth requirements for requesting a temporary exception from a WSU information security policy or standard. By allowing limited exceptions, WSU supports its goals of facilitating innovation and operational efficiency while safeguarding data and technology resources.
Information Security Risk Assessment	UPPM 87.25	Policy overview: Regular and systematic assessment for potential threats and vulnerabilities, including identifying, analyzing, and prioritizing risks, protects WSU's information systems and data. This policy sets forth roles, responsibilities, and requirements for information security risk assessments so that appropriate safeguards can be implemented and maintained, thereby strengthening the security of WSU's IT environment.

Configuration Management and Change Management	UPPM 87.30	Policy overview: Managing configuration and change activities protects the confidentiality, integrity, and availability of WSU institutional data and information systems. By establishing requirements for consistent configuration and change management practices, this policy provides a framework that enables WSU to maintain secure, reliable, and well managed IT environments.
Business Applications Security	UPPM 87.32	Policy overview: Establishing comprehensive security and privacy requirements for business applications used by WSU protects WSU's critical administrative, research, and academic systems. This policy ensures controlled access, secure development, proper data handling, and technical safeguards. Additionally, this policy mandates proper documentation, role accountability, vendor compliance, and user training to protect institutional data and maintain system integrity.
Encryption Security	UPPM 87.33	Policy overview: Robust encryption helps safeguard institutional information, including but not limited to research data, student records, and financial and personal information. This policy sets forth encryption requirements, including what types of data must be encrypted, methods of encryption, and compliance with industry standards and applicable laws
Wireless and Internet of Things Security	UPPM 87.35	Policy overview: Wireless networks provide unique advantages but also pose security and administrative challenges that necessitate a high level of technical coordination and adherence to strict requirements. This policy sets forth the roles, responsibilities, and requirements for ensuring the integrity of WSU's wireless networks.
Cloud Services, System Development, and Supply Chain Management	UPPM 87.37	Policy overview: Ensuring that third-party systems meet WSU's security and privacy requirements protects WSU's IT environment and data. This policy establishes the roles, responsibilities, and requirements for securely acquiring, developing, and managing cloud storage services, information systems, and other components used by WSU.
System Information Integrity	UPPM 87.40	Policy overview: Ensuring that WSU's systems and information are protected helps maintain a secure and reliable IT environment that supports WSU's academic, research, and administrative missions. This policy establishes the requirements to prevent, detect, and correct vulnerabilities across WSU's systems.
Anti Malware	UPPM 87.42	Policy overview: To protect the integrity and reliability of WSU's IT systems, WSU maintains and enforces a comprehensive anti-malware strategy requiring updated protection, centralized monitoring, and automated threat response, with additional controls for high-impact systems. This policy sets forth the standards and requirements for the effective implementation and oversight of WSU's anti-malware program.

Logging and Monitoring	UPPM 87.50	Policy overview: Effective logging and monitoring are essential to protecting WSU's information systems by enabling the timely detection of security events, misuse, and system anomalies. This policy establishes the requirements for logging and monitoring as well as generating, reviewing, and securing audit records to support operational oversight, incident investigation, and regulatory compliance.
Remote Access	UPPM 87.51	Policy overview: Ensuring secure and reliable remote access to WSU systems protects WSU data, facilitates WSU educational, research, and business operations, and is essential to support WSU's mission. This policy sets forth roles, responsibilities, and requirements for authorizing and managing remote access and ensuring the security of WSU's network and computer systems, including specific requirements for moderate- and high-impact systems.
Data Protection and Classification	UPPM 87.53	Policy overview: Institutional Information is a valuable WSU asset that must be categorized and safeguarded based on sensitivity and risk. By establishing clear requirements for all classifications of data, this policy ensures that Institutional Information is carefully managed, maintained, protected, and used appropriately throughout its lifecycle, as well as protected from unauthorized access or disclosure.
Information Security Incident Management and Breach Notification	UPPM 87.55	Policy overview: WSU is responsible for ensuring the privacy, confidentiality, integrity, and availability of its information systems, services, devices, and data. Establishing a consistent and coordinated approach to handling security incidents helps to minimize unauthorized access, misuse, loss, destruction, theft of information, and disruption of services that can be caused by information security incidents. Information gained and lessons learned during the incident response process may improve future responses to incidents, improve training, and help to build institutional resilience. Proper handling of information security incidents may mitigate potential harm to WSU's: • Strategic plan and business objectives; and • Financial operations, brand, and reputation. This policy provides a WSU-wide framework to help facilitate the development and implementation of consistent and coordinated procedures for reporting and responding to information security incidents across the WSU system.
Personnel Security	UPPM 87.60	This new policy lists requirements for appropriate screening, onboarding, monitoring, and departure procedures for personnel in order to protect WSU's information systems.
Physical Security	UPPM 87.62	Policy overview: Protecting the physical security of WSU facilities where IT systems are housed is critical to preventing unauthorized physical access, damage, or theft of WSU IT resources and information. By setting forth requirements for facility access, security, and environmental controls, this policy helps ensure the safety, security, and reliability of WSU's IT infrastructure.
Software Development	UPPM 87.65	Policy overview: All WSU software applications must be procured, designed, developed, used, and maintained in a manner that protects institutional data, systems, and user privacy. This policy establishes

		requirements to ensure that information security and user privacy considerations are integrated within the entire software development lifecycle.
Business Continuity and Disaster Recovery	UPPM 87.70	Policy overview: Business continuity and disaster recovery planning is a critical part of ensuring the security and reliability of WSU's information systems, as well as the protection of WSU data and information. This policy sets forth roles, responsibilities, and requirements for developing, maintaining, and testing contingency plans.
Data Retention Backup and Archive	UPPM 87.75	Policy overview: Protecting the confidentiality, integrity, and availability of WSU data and information requires robust data management and backup in accordance with all applicable laws, policies, and standards. This policy sets forth the roles, responsibilities, and requirements for creating and maintaining backup and archived system data.
Records Management	UPPM 90.01	This revision: • Changes policy name from "University Records – Retention and Disposition" to "Records Management"; • Removes inaccurate and outdated information regarding All-University and Unique Department Records Schedules, pending a complete overhaul of the policy that will be completed this summer; and • Adds links to currently posted retention schedules through the Secretary of State website.
Travel Management	UPPM 95.01	This revision: • Clarifies approval and exception processes to reflect Workday protocols; • Updates definitions and specifications for "out of state travel"; • Changes formatting to match current policy template; and • Updates links and resources throughout.
Travel Advance	UPPM 95.05	This revision: • Adds sections addressing advance repayment default; • Updates formatting to reflect current policy template; and • Updates links throughout.
Extenuating Circumstances During University Travel	UPPM 95.18	This revision: • Adds the purpose and applicability of the policy; • Clarifies expectations and procedures for travel alterations; • Clarifies coverage options for incurred medical costs; • Allows exceptions to cost of return; • Broadens coverage of the policy from injury/illness to extenuating circumstances; and • Changes the title from "Injury or Illness While on Travel Status" to "Extenuating Circumstances During University Travel".
International Travel	UPPM 95.53	This revision: • Clarifies process for requesting travel; • Requires that deans approve international travel; • Adds that expenses occurred prior to approval of Spend Authorization will not be reimbursed; • Updates information on student travel and the International Travel Registry; • Updates information on high-risk travel; and • Updates links throughout.