# University of New Mexico School of Law Information Technology Policies

## 1. Introduction

UNM has adopted comprehensive policies, standards and guidelines relating to information security and computer use. These policies supplement the University Administrative Policies and Procedures Manual found at http://policy.unm.edu. Specific applicable policies include:

UNM UBP 2030: Social Security Numbers
UNM UBP 2500 Acceptable Computer Use
UNM UBP 2520 Computer Security Controls and Guidelines
UNM UBP 2540 Student Email
UNM UBP 2550 Information Security
UNM UBP 2560 Information Technology Governance
UNM UBP 7215 Credit Card Processing

Additionally, the Office of the Chief Information Officer (CIO) has published IT Operational Procedures, Guidelines, and Standards including an Information Security Program. The CIO IT Standards are located at http://cio.unm.edu/standards/index.html#itprocedures.

### 1.1. Role of the School of Law Information Technology Department

The University of New Mexico School of Law (SoL) Information Technology (IT) department provides supplemental computing services to the law school community including students, faculty, and staff. The following policies apply to all persons who use School of Law computing and network resources. Additional School of Law IT policies and procedures include **Incident Management, Problem Management, Change Management,** and **System Access**. While these documents are for internal use only by the IT department, document review may be requested from the Assistant Dean for IT.

## 2. Purpose of this Policy

The purpose of the policy is:

- To establish an approach to the protection of the school's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.
- To prescribe mechanisms that will aid in the identification and prevention of abuse of data, applications, networks, and computer systems.
- To define mechanisms that will protect the information infrastructure of the School of Law and allow the school to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to University-wide resources.

## 3. Responsibility

The School of Law Dean or the Dean's designate and the Assistant Dean for Information Technology will ensure that:

- The information security policy is reviewed and updated on a regular basis and published as appropriate.
- Supervisors provide appropriate training to assigned staff, data custodians and users.
- School of Law Information Technology is responsible for security implementation, incident response, periodic user access reviews, and notification of users of network operations including information about virus infection risks.
- School of Law users are responsible for the safe handling, storage, and disposal of University data.

Violation of the Information Security Policy may result in disciplinary actions authorized by the University.

## 4. General Policy

While the School of Law IT does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the University's computing resources require the backup and storage of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendering of services.

UNM or School of Law IT may also specifically access and examine the account of an individual user if necessary to comply with federal or state law or if there is reasonable suspicion that a law or policy has been violated and examination of the account is needed to investigate the apparent violation as allowed in UBP 2500. When an employee separates from the School of Law, work-related files remain the property of the University.

Communications and other documents made by means of University computing resources are generally subject to New Mexico's Inspection of Public Records Act to the same extent as they would be if made on paper. Information stored electronically may also be made available in administrative or judicial proceedings; therefore, all employees are urged to use the same discretion and good judgment in creating electronic documents as they would use in creating written paper documents. The University will disclose illegal or unauthorized activities to appropriate University personnel and/or law enforcement agencies.

Vulnerability and risk assessment tests of external network connections should be conducted by School of Law IT on a regular basis.

Security reviews of server breaches of security will be conducted by School of Law IT on a regular basis. These reviews will include monitoring access logs and results of intrusion detection software, where used.

The University systems should not be used to host or generate data whose sole purpose is for commercial use. University hosted web sites fall under this same category and should not host commercial endeavors.

## 5. Use of Information Resources

The use of computing resources is a privilege and should not be taken for granted. The misuse or intentional destruction of computing resources is not acceptable use. If a computer or network resource in not functioning properly the user or supervisor should contact the School of Law Help Desk (277-8656 or email HELPDESK@law.unm.edu) for assistance.

## 6. Access Control

Data security policies are designed to allow the appropriate authorized user the appropriate system access. The School of Law recognizes that there is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes.

Access to the network and servers and systems will be achieved by individual and unique logins which will require authentication. Access to "shared" server folders may be requested by the shared folder owner; only the owner may request additional account holder access. In general, access to "home" folders and shared folders is granted using standard AD security groups and NTFS permissions.

- Only the shared folder owner may request modifications (adding or deleting) to the folder.
    - Permissions may be read only or modify and must be specified.
- All modifications must be requested by submitting a Helpdesk ticket for tracking purposes.
- Unused file shares may be archived; two copies must be created before the data is removed from the server.
    - Notice must be given to the law school community prior to any file share archiving.
- Remote access to School of Law servers is restricted except by IT Staff to a single server, using the secure RDP protocol.
- Remote access to home and shared folders may be requested as documented in **Section 6.2.1 Remote Access To Network Storage**.

Privacy and confidentiality of information is documented in **Section 10. Data Classification.**

### 6.1. Accounts

Users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users shall secure their username or account name, password, and system from unauthorized use. Sharing an account may result in suspension of account privileges. Employee account requests (faculty, staff, visitors, and student employees) are fulfilled using the School of Law's SharePoint Employee Onboarding workflow process and are completed within one business day. All new employees must

schedule 30-minute Computer Orientation training with the IT department. An account is created automatically for every law student upon entry into law school. All account holders must sign an account agreement form which is then filed within the SoL.

### 6.2. Usernames

Every School of Law user account has a username that is unique. Student usernames consist of the first six characters of their last name followed by the first two characters of their first name. Faculty, staff, visitors, and student employee usernames consist of the last name only whenever possible or the first initial of the first name appended to the last name if the account name is already in use. Student name change requests or changes in class status must be authorized by the Registrar. Faculty and staff account name changes may be granted by request after a qualifying life event (e.g. marriage or official legal name change). Students enrolled in the clinical law program are given a second clinic-specific account used only during enrollment in the clinic and retained in a separate address list. Clinic accounts are created as firstname.lastname@clinic.law.unm.edu. Usage and policies are covered in a separate document specific to the clinical law program. School of Law alumni are provided a new, permanent email address in the form of firstname.lastname@alumni.law.unm.edu. Email in the student account is not forwarded to the alumni account. The Career and Student Services department is responsible for communicating alumni account information to graduating students.

### 6.3. Passwords

Accounts are assigned a password when created and must be changed at first use. School of Law IT follows the UNM Password Standards. Passwords expire every 180 days. Passwords will not be sent in email unless they have been encrypted. If this is not possible, then another secure means must be used to communicate the password to the user. If you forgot your password, you must come to the IT office (Hart Wing, 3403) during normal business hours to request a password reset. IT Staff can change passwords over the phone provided you can verify your identity with your Banner ID number.

### 6.4. Email

Each account holder is provided an email address on the law school's Microsoft Exchange server. The email address currently takes the form of username@law.unm.edu. Aliases or alternative email addresses may be allowed with appropriate business need. Email forwards are provided for Adjunct faculty and Institute of Public Law staff only; Microsoft Outlook "rules" may be used for client-side forwarding to an alternative email address. The School of Law uses a Barracuda spam appliance for filtering unsolicited email. Potential spam is marked with [SPAM] in the subject line and delivered to the recipient. Occasionally, a valid sender's email will be incorrectly tagged as spam; the IT department can "white list" specific senders by request. The Barracuda appliance also scans for viruses and blocks or quarantines files with certain extensions including but not limited to: .adp, .bas, .bat, .cmd, .com, .dll, .exe, .js, .link, .msi, .pif, .rar, .reg, .scr, .vbs, and .zip.

### 6.4.1. Quota

All email accounts are provided with email quota based on current server resources. Three levels of quota are set: Warning, No Send, No Receive. Faculty and staff may request additional temporary quota increases due to travel or other extenuating circumstances. The IT department can help faculty and staff configure email archiving. Online archiving is available to all faculty and staff.

### 6.4.2. Usage Policy

All email communication is governed by UNM Business Policies and Procedures governing electronic management systems. Specifically, Policy 2510, Computer Use Guidelines, provides examples of prohibited communications:

- chain letters, pyramid schemes, and unauthorized mass mailings;
- fraudulent, threatening, defamatory, obscene, harassing, or illegal materials;
- non-work or non-class related information sent to an individual who requests the information not be sent;
- copyright law violation; and
- Commercial or personal advertisements, solicitations, promotions, destructive programs, or any other unauthorized use.

The Assistant Dean for Information Technology is responsible for monitoring email use. If an email violates UNM policy for electronic communications, the sender will be notified of the infraction. If the infraction continues, the School of Law Dean will be notified. Additional penalties may be imposed including locking the law school computer account. The law school will provide violators with a copy of UNM's Acceptable Computer Use policy in either electronic or hard copy form. Certain locking violations could also result in disciplinary action by the University or in criminal prosecution. Full email policy can be found on the School of Law's intranet here.

## 6.5. Backups

The IT staff performs daily backups of individual mailboxes. Mailboxes and individual email messages can be restored for approximately 30 days. Additionally, deleted account mailboxes are maintained on the mail server for up to 30 days and can be reattached to a new account.

## 6.6. Electronic Calendaring

The law school's standard email client, Microsoft Outlook, provides electronic calendaring. Users can grant scheduling access to other users and the IT department can create Outlook Public Folder Calendars for group scheduling.

## 6.7. Account Closure and Deletion

Accounts are deleted upon termination of employment, graduation, or students leaving the law school for other reasons. School of Law HR personnel are responsible for notifying IT if a faculty or staff member separates from the department. Student employee supervisors are responsible for notifying IT of student employee separations but in general, student employee accounts will be disabled after each semester unless arrangements have been made with IT. Law School graduates are given a grace period to study for the bar. December and May graduates accounts are deleted on or around August 1. Summer graduate accounts are deleted on November 1. Dual degree students do not retain their law school accounts past these days. Students are notified a week in advance of account disabling. Files associated with deleted accounts are retained only through the normal backup cycle unless otherwise requested by an employee's supervisor. A terminated or separated employee's supervisor may request access to the employee's files by submitting a written request to the Assistant Dean for Information Technology.

### 6.8. Account Revocation

A supervisor, Dean, or Senior Administrator may submit an email request that access to an account be revoked prior to formal separation from the School of Law. An account may also be temporarily locked by IT administrators in response to a suspected policy violation. Suspected policy violations and account revocation will be reported to the account holder. Account holders with revoked accounts may appeal the action by sending a written request for review to the School of Law Dean.

## 7. Network Storage

Each account holder is given a "Home" directory on a School of Law file server for network data storage. Additionally, shared file server space can be created for specific use. Users are strongly encouraged to store all work-related files on the file server as it is backed up on a daily basis. The IT department does not provide backup of workstations or laptops. Personal files must be stored on local hard drives and not on the file server. Certain file types are prohibited from network storage, including temporary files (~*.tmp), executables (*.exe), images (*.jpg and others) except those that are work-related, and music/video (*.mp3, *.mpeg4, and others).

### 7.1. Remote Access To Network Storage

Faculty and Senior Administrative staff may request remote access to their home directory or a shared folder by opening a ticket with the Helpdesk. Remote access is provided using Web Distributed Authoring and Versioning (WebDAV) folders. Only select shared folders are available for remote access.

### 7.2. Remote Access to Client Computers

UNM does not provide an Enterprise Virtual Private Network (VPN) connection to client workstations, therefore, School of Law computers may not be accessed off-site. Exceptions

to this policy are rarely granted and must be approved by the Assistant Dean for Information Technology.

### 7.3. Backups

Full server backups are performed on a weekly basis. Daily Differential server backups are performed during the week. Files stored on network drives for at least 24-hours can be restored from backup. Special arrangements can be made for long term storage; contact the IT department for more information. Current data retention periods are four weeks for full backups and two weeks for Differential backups.

## 8. Computing Hardware

The University has established a Strategic Partnership agreement with Dell and as such, the law school has standardized on Dell servers, workstations, laptops, and printers. All School of Law computing equipment purchases including scanners and other peripherals must be reviewed by the Assistant Dean for Information Technology.

### 8.1. Hardware Replacements

The School of Law follows a four-year computer replacement cycle for full-time faculty, staff, clinical law students, and the computer lab. Other computers are replaced (work study/student employees, emeritus faculty, Journals, and shared work spaces) with newer models as they become available. Faculty who wish to use their professional development or professorship funds for equipment purchases including computers and printers must coordinate the expenditure through the Assistant Dean for Information Technology. Procedures and guidelines are available in the Intranet's Faculty Handbook.

### 8.2. Hardware Support

The School of Law IT department provides support and service for School of Law-owned computing equipment including workstations, laptops, servers, printers. Support can be requested one of two ways, listed in order of preference:

- Email: helpdesk@law.unm.edu
- Help desk: (505) 277-8656

Due to the heterogeneous personal computer hardware environment and the expediency with which IT must provide service to faculty, staff, and students, we are unable to support or maintain any personal equipment beyond those services listed below:

- help with law school email
- help in configuring laptops to access file sharing, network printing services, and wireless network access
- assistance installing, testing and troubleshooting exam software provided by the School of Law
- help detecting and removing computer viruses, spyware, Trojans and adware

- general advice about possible causes of hardware problems and recommendations for third-party service providers
- assistance with personal computer purchases made through the UNM Dell Strategic Partnership

The School of Law IT department is housed in a secured area, with limited accessibility via "prox" cards administered by the Assistant Dean for Information Technology. Only IT and Media Center staff, the facilities coordinator, and the Law School Administrator are permitted 24/7 access. IT student employees are permitted access Monday – Friday, 7:30 AM – 5:30 PM. Law School students, faculty, staff, and others are permitted in the IT area only when resolving a technology issue or consulting with an IT staff member.

### 8.3. Loaner Laptop Checkout

The School of Law has a limited number of laptops available for short-term checkout by faculty, staff, and students. Laptops are available on a first-come, first-served basis. Students may not check out a faculty/staff loaner laptop unless the event is sponsored by a law school employee, and may not reserve or use the equipment post-commencement.

### 8.4. Local Administrator Access to Workstations

Due to the proliferation of viruses and Trojans, users are not given local administrator privileges to hard drives. Laptop users are given local rights but are not permitted to install software without the IT department's authorization.

### 8.5. Inventory

The IT department is responsible for maintaining timely and accurate inventory of all law school software licenses, workstations, laptops, printers, Media Center equipment, and computer peripherals (excepting mice, keyboards, cables, and similar lower-priced peripherals).

### 8.6. Mobile Devices

All policies governing confidential information and network security contained within this document apply to mobile devices (laptops, tablets, and smartphones) either UNM- or personally-owned, used to access School of Law data. A Mobile Tablet Policy for UNM-owned tablets is located in the Intranet's Faculty Handbook.

## 9. Software

### 9.1. Software Support

The law school uses a standard software image on all computers, allowing the IT department to quickly deploy new computers and resolve software issues. Therefore, no software may be installed on law school computers without permission from the IT department. If you have

software needs outside the standard image, please contact the IT department for future discussion. This includes all workstations and laptops on the law school Property Accounting inventory. Installation of non-UNM owned software is strictly prohibited. Software support is limited to installation, removal and resolution of problems or issues with functionality of software approved for use at the School of Law. Limited support is provided for software use questions.

Specific restrictions to personal computer support include:

- home visits
- support for personally-owned devices such as PDAs, most Smartphone's (see separate Smartphone policy), cameras, printers, and other computer peripherals
- off-campus Internet connectivity issues
- home network configuration including wireless networks
- operating system installation or repair
- data file backups
- software installation

### 9.2. Music and Movies

Copying music and movies is strictly prohibited. Copyright for acceptable software use and software copyright infringements are thoroughly covered in UNM UBP 2500. The Office of University Council has published numerous policies and information regarding copyrights on intellectual rights and main campus IT provides information on legal alternatives to pirating music and movies. Suspected infringements of this policy should be reported to the Assistant Dean for Information Technology or the School of Law Dean.

### 9.3. Printing

Networked printers and/or multifunction devices are provided in key locations throughout the building. Personal printer use is discouraged as the cost of expendables is significantly higher than network printing. Nuance Equitrac software is used for print release/management. See additional Intranet documentation on specific MFP use.

#### 9.3.1. Student Print Quota Policies

Students are provided a 625-page printing credit each semester. Unused printing allowance is not rolled over to the next term. Documents printed for the Clinic, faculty research, the Journals, and Moot Courts are exempt and do not count against the quota. Complete policies are located on the Intranet here.

## 10. Virus Protection

All workstations and laptops connecting to the Campus Data Communication Network (CDCN) must comply with the Rules of Use. Additionally, all workstations and laptops must have current virus scanning software installed and active. The School of Law IT department scans incoming

email for viruses and blocks or quarantines certain virus-prone attachment types including but not limited to: .adp, .bas, .bat, .cmd, .com, .dll, .exe, .js, .link, .msi, .pif, .rar, .reg, .scr, .vbs, and .zip. Main campus IT provides Symantec Endpoint Protection (SEP) free for all UNM students, faculty and staff with a valid NetID and Password. While antivirus software provides fairly good protection, the School of Law also recommends use of an anti-malware program such as MalwareBytes. Laptops connecting to the Enterprise Wireless network must follow the procedures set forth in the Network Access Control (NAC) guidelines. The School of Law considers all unauthorized file sharing using University resources to be virus-like activity. Intentionally accessing web sites that are known to contain virus-like activity without prior authorization is prohibited. System or network administrators will inform users when a virus has been detected if the software does not. The willful introduction of computer viruses or disruptive/destructive programs into the University environment is a crime, and violators are subject to prosecution. Users who repeatedly experience virus infections are subject to account locking and/or supervisor notification. Account holders with revoked accounts may appeal the action by sending a written request for review to the School of Law Dean.

## 11. Data Classification

All UNM Data must be assessed and classified according to its business or economic value to the University and its security/confidentiality requirements. The resulting classification will, in turn, facilitate applying the appropriate administrative, physical, and technical safeguards and security controls. The UNM Chief Information Officer (CIO) provides Data Classification Standards that all School of Law employees and students accessing UNM data must follow. No classified information including student, faculty and staff demographic, personal, or identifying data may be stored on removable media, laptops, or local hard drives. If School of Law email is set up on a personal or UNM-owned Smartphone or tablet, the device must be protected by a password and the phone or tablet should have a remote wipe feature in case it is lost or stolen. UNM-owned laptops and tablets will have Absolute Computrace, a tracking program, installed upon purchase. The IT department is responsible for managing Computrace and will work with the appropriate police department if a UNM-owned device is lost or stolen.

The IT department reviews School of Law servers on an annual basis to determine if Personally Identifiable Information (PII) or other confidential information is stored inappropriately. Due to the probability that the scanning software will identify “false positives”, the Assistant Dean will review the reports and will notify data owners if a violation is detected. The data owner must then take appropriate action to remove or encrypt the data.

## 12. Policy Violation

Noncompliance or violation of these policies will result in revocation of the privilege to access information resources and may also include other disciplinary action, pursuant to all Policies of the University of New Mexico. Violations may include, but is not limited to, the following:

- Any act that compromises information resource security.

- Intentional unauthorized access, use, destruction, alteration, dismantling, disfiguring, or disabling of any University information resource, including but not limited to intentional introduction of a virus.
- Disclosure of confidential information. This includes the sharing of passwords or leaving a workstation unattended while logged on in such a way that unauthorized transactions could be submitted.
- Disclosure of confidential or secured information in violation of FERPA or other state or federal rules or regulation.
- The use of data or other information resources for illicit purposes.

**12.1.** Unauthorized copying, storage or use of any software on any University computer in violation of the software licensing agreement.

### 12.2. Suspected Policy Violation Procedure

Any actual or suspected policy violation should be immediately reported to the Assistant Dean for Information Technology or the School of Law Dean. Complete and specific details of the incident should be included with the report. The IT department will either investigate the incident or will contact the University's Information Assurance office for assistance. Any breach, suspected breach, or security event or incident that could indicate a breach of PII will be reported immediately to UNM Information Security.

### 12.3. Appeal Process for Non-compliance

Individual appeals of any of the above for administrators, academic personnel, staff, and students must be made by the following steps:

- A written memo from the user must be provided to the School of Law Dean detailing the circumstances and the remedy to the policy violation.
- The Dean or the Dean's designate will obtain a written memo from the School of Law or main campus IT department detailing the policy violation and recommendations for remedy.
- The Dean or the Dean's designate will make a determination if the appeal holds merit and will notify the appellate of the decision.

### 12.4. Exceptions

In certain cases, compliance with specific policy requirements may not be immediately possible. In such cases, a written explanation of the compliance issue must be provided to the Assistant Dean for Information Technology for approval.

Approved March 2, 2016 by Sergio Pareja and Alfred Mathewson, Co-Deans