NEW MEXICO
LAW OFFICES OF THE PUBLIC DEFENDER

LOPD

Chief Public Defender
Bennett J. Baur

NMPD 500-004

Issue Date	6/18/2012
Effective Date	4/17/2024
Review/Revised Date	4/17/2024

This policy and procedure replaces any previous policies and procedures pertaining to Computer Information Systems, Internet, Intranet, Phone and Email Usage dated before the above effective date.

TITLE/AUTHORITY: Computer Systems, Internet, Intranet, and Email Usage
NMAC 1978, §1-12-10

REFERENCES: Department of Professional Standards for Email Use

PURPOSE: To set forth the responsibilities of department employees on proper use of the Information systems, the Internet, the Intranet, Phone, E-mail, VOIP (voice over internet protocol), and digital network and supporting systems

APPLICABILITY: All department employees

ATTACHMENTS: Department Professional Standards for Email Use Computer Information Systems, Internet, Phone Intranet and E-Mail Usage Policy Acknowledgement

DEFINITIONS:

1. Access – the ability to read, listen, change, or enter data using a computer or an information system.
2. Equipment – department computing equipment such as computers, monitors, keyboards, mice, routers, switches, hubs, networks, or any other information technology assets.
3. Freeware – software that is available free of charge and available for download from the Internet. Freeware may be protected by a copyright and is subject to applicable copyright laws.
4. Shareware – software that is initially available free of charge and available for download from the Internet. It requires a royalty fee to be paid to the designer for continued use and is protected by a copyright and is subject to applicable laws.
5. Information technology resources (IT resources) – computer hardware, software, databases, electronic message systems, communication equipment, computer networks , telecommunications circuits, and any information that is used by the department to support programs or operations that are generated by, transmitted within, or stored on any electronic media or computer system.

6. Security mechanism – a firewall, proxy, internet address screening or filtering program, or other system installed to prevent the disruption or denial of services and the unauthorized use, damage, destruction, or modification of data and software.
7. Sexually explicit or legally discriminatory – images, documents, or sounds that can be legally construed as discriminatory or harassing; defamatory or libelous; or obscene or pornographic; or threatening to an individual's physical or mental well-being; or read or heard for any purpose that is illegal; and
8. User means any person authorized by a state agency to access state IT resources, including a state employee, officer or contractor; a user for purposes of this rule does not include a person who accesses state telecommunications resources offered by the state for use by the general public.
9. Malicious code – any type of virus or type of code intended to damage, destroy, or delete a computer system, network, file, or data. Executable software, freeware, or shareware - a file or program which when initiated will process or complete the instructions contained therein.
10. Local Area Network (LAN) – a network of computers whose physical locations are close to each other. LANs are often used to share files and resources.
11. Wide Area Network (WAN) – a network of computers that spans a large geographic area, such as a state, province or country. WANs often connect multiple smaller networks or LANs.
12. Personally Identifiable Information (or PII) – information which can be used to distinguish or trace an individual's identity, such as their name, social security number, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual such as date and place of birth, mother's maiden name, etc.
13. Sensitive Agency Information – any confidential information, information system resources, data, records, PII, proprietary information, and other sensitive information handled by LOPD and protected by applicable laws, regulations or policies.

POLICY

1. Department employees shall abide by and familiarize themselves with NMAC 1978, § 1-12-10 Internet, Intranet, Email and Digital Network Usage.
2. Department employees shall use department computer resources, email and Internet solely for official department and state business, or as explained under "Procedure" in section 5(a) below.
3. All state of New Mexico policies relating to intellectual property protection, privacy, misuse of state equipment, sexual harassment, sexually hostile work environment, data security, and confidentiality shall apply to the use of IT resources.
4. Prohibited Internet Use
    a. No software licensed to the state nor data owned or licensed by the state shall be uploaded or otherwise transferred out of the state's control without explicit authorization from the agency head.
    b. Users shall not download executable software, including freeware and shareware, unless it is required to complete their job responsibilities and with authorization by the Director of IT.

c. Users are prohibited from accessing or attempting to access IT resources for which they do not have explicit authorization by means of user accounts, valid passwords, file permissions or other legitimate access and authentication methods.

d. Users shall not use state IT resources for illegal activity, gambling, or to intentionally violate the laws or regulations of the United States, any state or local jurisdiction, or any other nation.

e. No department employee shall utilize department IT resources to engage in political activity.

f. Department employees shall not use state equipment to download or distribute pirated software or data.

g. Department employees shall not display or transmit sexually explicit materials or reproduction of sexually explicit sounds on any department information system unless authorized as part of their duties and a written exemption from their District Defender and the Director of IT is obtained.

5. Users shall have no expectations of privacy with respect to state IT resource usage. Disciplinary action up to and including termination of employment or contract may result from evidence of prohibited activity.

PROCEDURE

1. Employees' Declaration

a. The department shall provide all employees withcomputer systems access with access to the Department Computer Information Systems, Internet, Intranet and E-mail Usage Policy.

b. All department employees who receive the Computer Information systems, Internet, Intranet, and e-mailUsage Policy shall sign a statement indicating they have reviewed and read the policy. The department shall keep the signed statement on file with Human Resources pursuant to retention policies.

2. Enforcement

a. Department employees shall have no expectation of privacy with respect to internet, e-mail usage, VOIP (voice over internet protocol) call logs and recorded messages, security access logs, or any files stored on department computers and/or servers.

b. The department has software that allows monitoring and recording of all e-mail, internet usage, VOIP and web sitevisits.

c. The department retains the right to record or reviewall visits to every web site, chat room, newsgroup, e-mail messages, phone calls, or file transfers.

d. The department may collect usage statistics about bandwidth usage and time spent on the Internet.

e. The department maintains data file storage on department servers and reserves the right to inspect any files stored on any department-owned computers, servers, hand-held devices, cell phones, laptops and any other data storage devices.

3. Compliance with Laws

a. Department employees shall respect the copyrights, software licensing rules, property rights, privacy,and prerogatives of others, as in any business dealings.

   b. Department employees shall only use downloaded files or software in ways that are consistent with licenses or copyrights.
   c. Department employees shall not upload any software licensed to the department or data owned or licensed by the department except as required by job duties.
   d. Unauthorized software or files downloaded via the Internet onto department computers become the property of the department.
   e. Software and hardware not purchased by the department will not be installed on department computers.
4. Sexually Explicit Material
   a. An employee who requires the display or use of sexually explicit material, which falls within legitimate job responsibilities, must obtain an exemption in writing from their District Defender and the Director of IT.
5. Permissible Internet Use
   a. Department employees may use the Internet for non-business research or browsing during mealtime or outside of working hours provided that all other requirements are met.
6. Security
   a. Department employees shall keep passwords and user identifications for department computer information systems, internet, and e-mail access confidential.
   b. Department employees shall comply with Department implemented IT security protocols and shall ensure any device or equipment necessary or required to access other Department equipment, servers, internet, etc. is secure and not shared.
   c. Department employees shall ensure the protection of all Sensitive Agency Information as required by privacy and confidentiality laws and regulations and by LOPD policy, procedures and practice regarding information security. IT resources shall not be used to reveal confidential or sensitive information, client data, or any other information covered by existing state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms. Users shall not engage in the unauthorized release of confidential information, personally identifiable information (PII) or sensitive agency information via IT resources, including but not limited to newsgroups, social media, or chat rooms.
   d. Department employees shall not attempt to disable, defeat, or circumvent any department security mechanism.
   e. Department employees shall take appropriate action to protect LOPD equipment from damage, loss or theft. Employees shall immediately notify their supervisor of any damage, loss or theft of equipment.
7. Sanctions
   a. Any violation of these policies is grounds for disciplinary action or other sanctions, up to and including dismissal or termination.

______________________________ Date: 4/16/2024

Bennett J. Baur
Chief Public Defender

Professional Standards for Email Use

The following are some guidelines regarding professional e-mail conduct and suggestions to avoid miscommunication. Digital miscommunication happens because we don't have access to the non-verbal cues, including tone of voice, body language, and facial expressions that give us valuable emotional context when we're discussing in person.

1. **Include a greeting in all emails.** Emails that do not include a greeting are easily viewed as rude. It only takes a few seconds to type, "Hi John" or "Dear Ms. Smith". Take the time to show the recipient of your email respect, by addressing them by name in a professional manner.
2. **Be professional, not sloppy.** Your colleagues may use commonly accepted abbreviations in e-mail, but when communicating with external customers, everyone should follow standard writing protocol. Your e-mail message reflects on our department, our clients, and state employees so traditional spelling, grammar, and punctuation rules apply.
3. **Keep messages brief and to the point.** Just because your writing is grammatically correct does not mean that it has to be long. Nothing is more frustrating than wading through an e-mail message that is twice as long as necessary. Concentrate on one subject per message whenever possible.
4. **Realize typos send a message.** Typos reveal that we were in a rush or heightened emotional state when we hit send (or that we're the boss, and don't need to care about typos). Even if you're in a rush, it's best to spend those extra two minutes proofreading your work, or better yet, read it out loud to catch any typos your eyes quickly skip over when reading it in your head.
5. **Be sparing with mass e-mails.** Send group e-mail **only** when it's useful to every recipient. Use the "reply all" button only when compiling results requiring collective input and only if you have something to add. Recipients get quite annoyed to open an e-mail that says only "Me too!"
6. **Use the subject field to briefly indicate content.** Don't just say, "Hi!" or "From Laura." Every message should contain a short phrase to give notice of the content of the email. Do not put in lengthy sentences into your subject line. Many email viewers only show a short subject line for recipients.
7. **Use sentence case.** USING ALL CAPITAL LETTERS LOOKS AS IF YOU'RE SHOUTING! Using all lowercase letters looks lazy. For emphasis, use asterisks or bold formatting to emphasize important words. Do not, however, use a lot of colors or graphics embedded in your message, because not everyone uses an e-mail program that can display them.
8. **Don't use e-mail as an excuse to avoid personal contact.** Don't forget the value of face-to-face or even voice-to-voice communication. E-mail communication is not appropriate when sending confusing or emotional messages. Face-to-face is the preferred method of respectful communication.
9. **Remember that e-mail isn't private.** State employees have been fired for using e-mail inappropriately. E-mail is considered department property and can be retrieved, examined, and used in a court of law. Unless you are using an encryption device (hardware or software), you should assume that e-mail over the Internet is not secure. Never put in an e-mail message anything that you wouldn't put on a postcard.
10. **Don't send virus warnings or junk mail.** Always check a reputable antivirus Website or check with the LOPD IT department before sending out an alarm. Direct personal e-mail to your home e-mail account.
11. **Remember that your tone can't be heard in e-mail.** Have you ever attempted sarcasm in an e-mail, and the recipient took it the wrong way? E-mail communication can't convey the nuances of

verbal communication. In an attempt to infer tone of voice, some people use emoticons, but use them sparingly so that you don't appear unprofessional.

12. **Use a signature that includes contact information.** To ensure that people know who you are, and how to contact you, include a signature line that has your contact information, including your mailing address, Website, and phone numbers.
13. **Emotionally proofread your messages.** Typos are not the only thing you should be proofing your messages for. Always re-read what you've written before hitting send to make sure your message is clear and conveys the intended tone. Sending "Let's talk" when you mean "These are good suggestions, let's discuss how to work them into the draft" will make the recipient unnecessarily anxious. It's easy for emails or messages to be perceived as passive aggressive in tone. Imagine how you'd feel if you got a message that said, "Per my last email, just following up" or "Help me understand."
14. **Punctuation marks matter even more for one-word or very short sentences.** Responding "Okay." with a period can come across as more negative in tone than "Okay" without a period. Adding a period adds a finality to your statement and heightens the negative emotion. It can communicate, "This conversation is over" rather than "Okay, sure, we're in agreement." As you get to know someone, pay attention to their punctuation style.
15. **Don't panic.** If an email makes you enraged, anxious, or euphoric, wait until the next day to write back. Even better, talk face-to-face when you've calmed down. Once you've calmed down, you'll be able to better articulate your emotions, and the needs behind your emotions, rather than just your immediate reactions. When you do reply, re-read your draft through the other person's eyes. It might be easier to imagine how your reader will interpret your email if you first send it to yourself. (Additional tip: always leave the "To:" field blank until you're ready to hit send.
16. **Avoid email when you need a "yes."** An in-person request is more than thirty times more successful than an emailed one. Research shows people see email asks as untrustworthy and non-urgent.

500.004 NM Public Defender

Computer Information Systems, Internet, Intranet, Phone and E-Mail Usage Policy Acknowledgement Form

Employee Name (Printed): ______________________________

Job Title (Printed): ______________________________

Applicability: To be completed by all users of department phone, and computer information systems (employees, contractors, interns, volunteers, etc.) and filed with Human Resources in the employee's official personnel file by emailing the completed form to LOPD-HR.

Information System Access

- I have read the Computer Systems, Internet, Intranet, Phone, and Email Usage policy pertaining to proper usage of computer information systems, Internet, email, VOIP (voice over internet protocol), and general information regarding security. I fully understand these policies and agree to abide by them as a condition of employment.

- I understand that the user identifications and passwords issued to me allowing access to the various state and departmental information systems and any sensitive department information or personally identifiable information (PII) are confidential and are solely for my own use in carrying out my job responsibilities. I will not divulge, loan or in any way make this information available in any form to any other individual.

- I understand that documents, files or programs I create for the department, on department time, or using department resources are the property of the department.

- I also understand that the department reserves the right to review, audit and inspect, at its discretion, any documents, files, emails, or material resident on computers, servers, phones, VOIP (voice over internet protocol) call logs and recorded messages, laptops, and any other data storage devices or media owned by the department, even if protected by individual password. I further understand that the department's security and monitoring software may record email and every network and internet transaction from my department equipment or transmitted over department communication lines.

- I understand that the department reserves the release of state confidential information, the loss of information systems data, loss or damage of equipment through my failure to comply with these requirements or any unauthorized use of my access may subject me to disciplinary action, up to and including termination.

____

Employee Signature Date