UKPEAĠVIK IÑUPIAT CORPORATION

UIC CORPORATE HANDBOOK

INFORMATION TECHNOLOGY USE AND SECURITY POLICY

UIC-IT-2-6-008 Rev. 2

PURPOSE

The purpose of this policy is to enable UIC to:

- Outline the acceptable use of its information systems, and
- Set rules to protect UIC and its employees.

Inappropriate use of IT assets and systems exposes UIC to risks including malware attacks, comprise of network systems and services, and legal issues. In general, acceptable use covers everything respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements.

SCOPE

This policy applies to all employees, Board of Directors, contractors, consultants, and temporary employees at UIC and its subsidiaries, including all personnel affiliated with third parties, that use UIC's information systems. This policy applies to all information equipment and assets that are owned or leased by UIC and other information equipment that may be used to access UIC's information systems.

POLICY STATEMENT

This policy is to protect UIC's information, assets, and IT resources while reflecting UIC's established culture of openness, trust, and integrity. This policy is intended to promote security best practices among UIC's employees and those with whom UIC collaborates. Protecting UIC's information, physical, and IT resources is a team effort involving the participation and support of every UIC employee and affiliate who interacts with information and/or information systems. It is the responsibility of every employee to know and comply with these guidelines.

DEFINITIONS

a. Information Systems – These are Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, mobile devices, software, operating systems, storage media, network accounts, and systems used for collecting, creating, storing, processing, and distributing information.

b. Information – Anything spoken, overheard, written, stored electronically, copied, transmitted, or held intellectually concerning UIC's general business, information systems, employees, business partners, or customers, including data and entity types.
c. Employees – Employees include full-time employees, part-time employees, and any authorized personnel having access to UIC's information systems.
d. User – Employee authorized to have access to a designated information system.
e. Data – One or more of the following characterize data as used in this policy:
    i. Information that is processed by means of equipment operating automatically in response to instructions given for that purpose
    ii. Information that is recorded with the intention that it should be processed by means of such equipment
    iii. Information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system
    iv. Information that does not fall within any of the above but forms part of a readily accessible record pertaining to an individual

    Data, therefore, includes any digital data generated by a computer or automated equipment and any physical information that is part of a relevant filing system.
f. Authentication Token – A smartphone app (e.g., Microsoft Authenticator) or hardware key used to provide additional security when logging into a system. Also known as multifactor authentication (MFA) tokens.

RESPONSIBLE PARTIES

a. All users are required to adhere to this policy while using any of the company's information systems. Users are responsible for conducting themselves in a professional, responsible, and courteous manner at all times.
b. Managers are required to inform all employees of this policy and ensure each employee fully understands and undertakes to comply with this policy.

COPYRIGHT AND OWNERSHIP

a. Users should be aware that the data they transmit or create on company systems is deemed to be the property of UIC and is subject to monitoring. UIC proprietary information stored on electronic and computing devices whether owned or leased by UIC, the employee, or a third party, remains the sole property of UIC.
b. All software, files, spreadsheets, calendars, work products, messages, memos, or any other data created and/or stored on company equipment are deemed the property of UIC.

c. Employees must ensure that proprietary information and equipment is protected in accordance with this policy, and must promptly report theft, loss, or suspected misuse of company information or equipment.
d. The company has the capability, and retains the right to access data, electronic and voice mail messages, Internet usage history, etc., at any time, with or without users' specific consent or knowledge. This is necessary to implement monitoring and compliance with UIC's information assets.
e. For security and network maintenance purposes, authorized individuals within UIC may monitor equipment, systems, and network traffic at any time.
f. Employees have no expectation of privacy in any files, data, photos, or any other information stored in any manner on any of the company's information assets and expressly acknowledge that any and all such information and files are the property of the company and may be deleted, shared, copied and/or destroyed at the company's sole and absolute discretion, without any liability whatsoever to the employee, or former employee.

ACCEPTABLE USE

General Use of Company Resources

Users are required to adhere to the following principles regarding the use of company information systems:

a. Employees may use only computers, computer accounts, and data for which they have authorization. Employees and/or Managers are required to notify IT immediately if their authorizations are no longer required for their current or new position.
b. Each user is required to maintain the confidentiality of their authentication information (i.e., usernames, passwords, and MFA tokens/apps) and to secure resources against unauthorized use or access. If the security of a password or MFA token is in doubt, it should be changed immediately.
c. Employees are not to reuse their passwords for external websites or services.
d. Use of any group/shared authentication information must be approved by the Senior Director of IT and be maintained solely among the authorized members of the group.
e. Employees should use UIC-provided hardware and software without altering any configuration settings implemented by the IT department. Any modification of the configuration may expose UIC's network and information resources to unauthorized access from users.
f. Employees may not acquire hardware, software, or services (including cloud services or other subscription-based services) prior to consulting IT.

g. Software (including shareware) shall not be installed on laptops or desktop computers, without first requesting approval through the IT department's established request process. This applies to company-provided laptops, desktops, and other information systems approved by UIC IT.

h. Each user is personally responsible for the information security aspects relative to his or her laptop or desktop computer, or mobile device, and must comply with corporate security policies.

i. Employees are personally responsible for protecting their laptops and mobile devices against theft and for secure storage of information stored on them. Authorized external hard drives, removeable USB drives and other external storage devices will not include any personal identifiable information (PII) or other employee data, without the previous written approval of IT.

j. Employees shall use the company's e-mail and other electronic communication assets in accordance with the UIC Online Communications and Social Media Policy.

k. When handling information, whether electronically or in hardcopy, employees shall take into consideration the information's classification and safeguard it appropriately based on the information security requirements of the classification level.

l. Sensitive or controlled information may only be stored in approved locations. This includes but is not limited to:

   i. Company proprietary data
   ii. Personal identifiable information (PII)
   iii. Financial/banking information
   iv. Government-regulated data, such as Controlled Unclassified Information (CUI)

   CUI is subject to additional restrictions as per UICGS-SECU-1-6-024 (CUI Handling Policy).

Personal Use

a. The company provides a variety of electronic tools to its employees to assist them in meeting the business objectives of the company. Incidental, limited, personal use of reasonable duration may be permitted if it does not interfere with a system's intended business purpose.

b. Users are responsible for exercising good judgment regarding the reasonableness of personal use.

c. Users are not to process, store, or directly access UIC data information on systems, other than those provided by UIC.

d. Users are not to copy, export, or upload UIC data to any personal device, removable storage, or cloud hosted server without the written consent of the UIC Senior Director of IT.

e. Users are not to sign up for non-business-related websites, services, or mailing lists using their company-provided email address

f. Examples of sites and activities that are expressly prohibited include, but are not limited to:
   i. Pornographic or sexually oriented sites
   ii. Internet sites or social media dedicated to violence or hatred
   iii. Internet relay chat (IRC) or illegal chat rooms
   iv. MP3 downloads and file sharing or streaming media sites

Adherence with Federal, State, and Local Laws

The nature of UIC's business requires it and its employees to adhere to a country's federal, state, and local laws. This is applicable to all subsidiaries of UIC operating outside the jurisdiction of the United States. All employees of UIC are expected to uphold federal, state, and local laws.

UNACCEPTABLE USE

Under absolutely no circumstance are any UIC's systems to be used to solicit, harasses, or otherwise offend, nor may it be used for any unlawful purpose, such as accessing illegally distributed materials that are sexually explicit or otherwise inappropriate or unlawful.

The following activities are, in general, prohibited. At UIC's sole discretion, employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., IT staff may have a need to disable the network access of a host that is disrupting production services).

a. Prohibited system and network activities include:
   i. Unauthorized copying of copyrighted material
   ii. Installing or using peer-to-peer (P2P) applications
   iii. Streaming audio or video media for personal use over corporate facility internet
   iv. Exporting software, technical information, or encryption software or technology
   v. Introduction of malicious programs into a company network or server
   vi. Revealing your account password or authentication device to others or allowing use of your account by others
   vii. Making any offers of non-company products, items, or services

  viii. Enabling security breaches or disruptions of network communication

  ix. Circumventing user authentication or security of any host, network, or account

  x. Providing information about, or lists of, any company employees to parties outside the company

b. Prohibited e-mail and communications activities include:

  i. Sending unsolicited non-work-related e-mail messages, including but not limited to junk mail or spam

  ii. Any form of harassment via electronic mail, online communication, or telephone

  iii. Unauthorized use, or forging, of e-mail header information

  iv. Auto-forwarding email to a non-company address

c. Employees may not connect any device to the company's internal network unless the device is owned by the company and approved and managed by UIC IT. Guest and Mobile Wi-Fi networks are provided for this purpose.

d. Employees may not store, process, maintain, or backup company data on personally owned computers, mobile devices, or any storage device not owned by UIC without the approval of the company's senior leadership and the UIC Senior Director of IT. If any such unauthorized storage, processing, maintenance or backups occur, such company data shall retain its character as a company asset and shall remain company property.

e. Employees may not share, store, or transfer company data using any cloud service platform (e.g., Dropbox, Google Drive, iCloud, etc.) without the approval of the company's senior leadership and the UIC Senior Director of IT. This includes instances of Microsoft 365 not owned by UIC.

f. Employees may not upload, share, or discuss any company proprietary, confidential, or controlled information with Generative Artificial Intelligence (AI) chat platforms (e.g., ChatGPT, Copilot, Gemini, DeepSeek, etc.) that are not approved by the company's senior leadership. This includes but is not limited to:

  i. CUI

  ii. PII

  iii. Financial/banking information

  iv. Intellectual property

  v. Customer or employee data

  vi. Any other sensitive information that could compromise UIC's interests or privacy obligations

g. Employees may not use AI chat platforms for activities that violate any UIC policy.

h. Employees may not engage in conversations or tasks on AI chat platforms with the intent to circumvent established business processes, security protocols or data protection measures.
i. Use of company equipment to copy and/or transmit any document, software, or other matter in violation of any copyright, patent, or any other applicable intellectual property right, law, or regulation is strictly prohibited.
j. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) constitutes harmful behavior and is unacceptable as per company policy.
k. Revealing account passwords to others or allowing use of accounts by others is prohibited. This includes family and other household members when work is being done at home.
l. Executing any form of network monitoring that will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty, is not allowed.
m. Employees should not circumvent security or user authentication on any company device.

POLICY COMPLIANCE

The UIC Information Technology department will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Any violation of this policy will be handled in accordance with the UIC Corrective Action Policy (UIC-HR-2-6-026) which may result in disciplinary action, up to and including termination.

EXCEPTIONS AND DEVIATIONS

The UIC Senior Director of IT, in consultation with Executive Management as necessary, must approve any exception to this policy in advance.

UKPEAĠVIK
IÑUPIAT
CORPORATION

UIC CORPORATE HANDBOOK

REVISION HISTORY

Revision	Change Description	Author / Revised By	Approved By	Effective Date
1	Original issue	Ted Rayhart, UIC Senior Director of IT	Delbert Rexford, CEO/President	6/30/2020
2	Policy Update	Ted Rayhart, UIC Senior Director of IT	Dr. Pearl K. Brower, CEO/President DocuSigned by: Pearl Brower 4F40BFC21C1549F...	5/5/2025