HO-CHUNK NATION CODE (HCC)
TITLE 6 – PERSONNEL, EMPLOYMENT AND LABOR CODE
SECTION 4 –TECHNOLOGY RESOURCES USAGE ACT

ENACTED BY LEGISLATURE: 4/29/08

LAST AMENDED: January 18, 2022

CITE AS: 6 HCC § 4

This Act supersedes the Ho-Chunk Internet & Intranet Usage Act adopted by Legislative Resolution 4/11/00D and restated on 10/25/01and restated and renamed on 5/22/07.

TABLE OF CONTENTS

1. **Authority**.

a. Article V, Section 2(a) of the Constitution grants the Legislature the power to make laws, including codes, ordinances, resolutions and statutes.

b. Article V, Section 2(f) of the Constitution grants the Legislature the power to set salaries, terms and conditions of employment for all government personnel.

c. Article V, Section 2(h) of the Constitution grants the Legislature the power to enact all laws prohibiting the regulation conduct and imposing penalties upon all persons within the jurisdiction of the Nation.

d. The Ho-Chunk Nation Employment Relations Act (ERA) (6 HCC § 5) prescribes policies and procedures for employment conduct, discipline, and workplace conditions.

2. **Purpose**. This Act establishes the rules for the acceptable use of the technology resources of the Nation. These rules are in place to protect the users and the Nation. Inappropriate use exposes the Ho-Chunk Nation to risks including cyber-attacks, compromise of network systems and services, and legal issues.

3. **Scope**. This Act applies to all employees, contractors, outside organizations and consultants and other workers of the Nation, including all personnel affiliated with third parties in their use of the Nation's technology equipment and software or in doing work for the Nation. Technology equipment includes, but is not limited to, computer, printers, removable media, cameras, scanners, and digital equipment.

4. **Overview**.

a. The Ho-Chunk Nation recognizes the responsibilities of the Nation and its employees to each other and to the public and, as such, prescribes rules to ensure fair and consistent conditions of employment for all. Technology services are employee user's privilege to enhance workplace productivity. These services must be used judiciously and professionally to ensure it supports achievement of the desired goals and objectives of the Nation.

b. This Act is not intended to impose restrictions that are contrary to the Ho-Chunk Nation's established culture of openness, trust and integrity. The Nation is committed to protecting the Nation and its employees and partners from illegal or damaging actions by individuals or outside organizations, either knowingly or unknowingly.

c. Technology systems, equipment and software are the property of Nation. These resources are to be used for business purposes in servicing the interest of the Nation, its members, clients and customers in the course of normal operations.

d. Effective security is a team effort involving the participation and support of every Ho-Chunk employee and affiliate who deals with information and/or information systems. It is the responsibility of every technology user to know these guidelines and to conduct their activities accordingly.

e. To further assist users with their technology needs the Ho-Chunk Nation has created the Division of Information Technology (IT) formerly known as the Department of Management Information Systems.

5. **Declaration of Policy**. All users of the Nation's technology resources will adhere to this Policy and each Supervisor will enforce this Policy. This Policy will be incorporated as a directive in the Nation's Employment Relations Act.

6. **Personal Computers and Devices** Using personally owned computing equipment, laptops, and software in the workplace for Ho-Chunk Nation business is prohibited. For purposes of the preceding sentence the term "personally owned computing equipment" shall include laptops, camera, flash drives (usb drives), external hard drives, ipods and all other mass storage devices. This prohibition may be waived if a user receives permission to use said equipment from their immediate supervisor or from the Executive Director of their Department, provided that any employee using personal equipment take all reasonable efforts to secure the Nation's data security, follows any guidelines which their supervisor and/or Executive Director establish, including but not limited to the data storage of any work product, and upon ending employment with the Nation all data is removed from the employee's personal equipment by the IT Department.

7. **General Use**.

a. While the Nation's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the Nation's systems remains the property of the Nation. Because of the need to protect the Nation's network, network administrators will have access to manage any information stored on any network device.

b. Personal Use.

(1) Technology systems are property of the Ho-Chunk Nation. Users are responsible for exercising good judgment regarding the reasonableness of use. Individual departments may create guidelines concerning personal use of technology systems that are consistent with this Policy.

(2) Users should consult their Supervisor or manager if there is any question on the appropriateness and permissible use of the Nation's technology systems.

(3) For security, network maintenance, and compliance purposes, authorized individuals within Ho-Chunk Nation may monitor equipment, systems and network traffic at any time.

(4) Misuse of the technology resources and services will be considered employee misconduct for the purposes of disciplinary action.

c. Posting by users from a Ho-Chunk Nation e-mail address or account to newsgroups and social media is strictly prohibited, unless the posting is in the course of official business duties. For purposes of this paragraph, a newsgroup is a repository for messages posted from many users at different locations and usually involves a group discussion.

d. All messages and other electronic records created, stored, transmitted, or received using Ho-Chunk Nation resources are primarily for business purposes consistent with the interests of the Nation, its members, clients and customers in the course of normal operations.

(1) The Ho-Chunk Nation reserves the right to monitor the content of any record, non-record, document, or message created, stored, transmitted or received using the Ho-Chunk Nation's computers.

(2) While the Nation's network administration desires to provide a reasonable level of privacy, users should not expect any right to privacy when it comes to messages, records or non-records. The Ho-Chunk Nation reserves the right to monitor the content of any record, non-record, document, message created, stored, transmitted or received using the Ho-Chunk Nation's technology resources.

8. **Security and Proprietary Information**.

a. Proprietary Information.

(1) Examples of proprietary information includes but is not limited to the Nation's financial data, enrollment information, child and family information under provisions of Title 4 (Children, Family, and Elder Welfare Code) of the Ho-Chunk Nation Code (HCC), medical records and related information, business strategies, competitor sensitive information, trade secrets, specifications, customer lists, research data, and such other information that may be from time to time deemed proprietary, i.e., governmental negotiations.

(2) Proprietary information will be considered confidential and privileged.

(3) Unless a Supervisor states otherwise, users creating information are responsible for determining if the information is proprietary. Individuals creating proprietary information are responsible for marking electronic and paper copies in accordance with paragraph (4), below.

(4) Unless a Supervisor states otherwise, all material containing proprietary information will be clearly marked "Confidential." An exception to this rule is the release of financial data provided to Tribal members at District Meetings. This material will be clearly marked "For Tribal Use Only" and not for further release.

(5) Material marked "Confidential" will only be distributed to other employees or outside agencies on a need-to-know basis. Users providing unauthorized access to proprietary information may be subject to employee discipline as provided in the Nation's Employment Relations Act (6 HCC Sec. 5).

b. Protective Measures.

(1) Passwords will be kept secure and accounts will not be shared. Authorized users are responsible for the security of their passwords and accounts and will have their own individual password. System level passwords will be changed quarterly and user level passwords shall be changed every sixty (60) days.

(2) All Nation owned unattended technology equipment will be logged off or secured with a password when not in use.

(3) Encryption of information will be used in compliance with IT and other facility's acceptance encryption use policy.

(4) All equipment connected to the Ho-Chunk Nation Internet/Intranet/Extranet, will be continually executing approved virus-scanning software with a current virus database, unless overridden by IT directive.

(5) All users will use extreme caution when opening e-mail attachments received from unknown senders which may contain malware.

(6) Because information contained on portable equipment is especially vulnerable, special care should be exercised to secure these devices.

9. **Unacceptable Use**. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. Users may be exempt from these restrictions during the course of the legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of equipment disrupting production services). Violations of any of the below restrictions or prohibitions may subject the employee to disciplinary action up to and including termination. Unless specially noted, disciplinary action will be conducted pursuant to the Nation's Employment Relations Act (6 HCC Sec. 5). In addition, if warranted by the actions, violations of these policies may subject the employee to legal prosecution by Tribal, State and Federal officials.

a. General Restrictions.

(1) Misuse of technology systems that is adverse to the interests of the Nation is prohibited.

(2) The authoring, forwarding, viewing, or sending of graphic nudity, obscene, or pornographic material and the use of obscenity or profanity is strictly prohibited.

(3) The use of Nation technology resources or systems for personal internet gambling is strictly prohibited.

(4) The use of the Nation's systems for financial gain or anything of substantial value for private benefit is strictly prohibited.

(5) The unapproved or unlawful release of confidential or proprietary information belonging to the Nation using technology systems is strictly prohibited.

(6) Under no circumstances is an employee of the Ho-Chunk Nation authorized to engage in any activity that is illegal under Tribal, Local, State, Federal or International law

while utilizing Ho-Chunk Nation technology equipment and systems.

b. Restricted System and Network Activities. The following activities are strictly prohibited, with no exceptions:

(1) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Ho-Chunk Nation.

(2) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Nation or the end user does not have an active license is strictly prohibited.

(3) Exporting software, technical information, encryption software or technology, in violation of International or Regional Export Control laws, is illegal. IT should be consulted prior to the export of any material that is in question.

(4) Introduction of malicious programs or malware into technology systems.

(5) Revealing one's account password to or allowing use of one’s account at any time by any individual, including but not limited to, supervisors, co-workers, friends, family members or other household members.

(6) Using a Nation owned technology resource to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

(7) Making fraudulent offers of products, items, or services originating from any Ho-Chunk Nation account.

(8) Making statements about a warranty, express or implied, unless it is a part of normal job duties.

(9) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data for which the user is not an intended recipient or using an account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this paragraph, "disruption" includes any intentional activity causing disruption of service or network communication for malicious purposes.

(10) Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.

(11) Executing any form of network monitoring which will intercept data not intended for the user’s device, unless this activity is a part of the user’s normal job/duty.

(12) Circumventing user authentication or security of any device, network or account.

(13) Interfering with or denying service to any user other than the user's device unless this activity is part of the user's normal job duty.

(14) Unless authorized in writing by a Supervisor and the user's Executive Director or necessary to accomplish a function of work, providing information about, or lists of, Ho-Chunk Nation employees to parties outside the Ho-Chunk Nation.

c. Restricted E-mail and Communications Activities.

(1) Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam), unless necessary to accomplish a function of work.

(2) Sending, forwarding, or responding to unsolicited, non-job-related e-mail or communications for, or in support of, outside organizations that are non-charitable, commercial in nature, or otherwise unsupported by the Nation.

(3) Any form of harassment via e-mail, telephone or other communication methods, whether through language, frequency, or size of messages.

(4) Unauthorized use, or forging, of e-mail header information.

(5) Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

(6) Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.

(7) Use of unsolicited e-mail originating from within the Nation's networks or other technology service providers on behalf of, or to advertise, any service hosted by the Ho-Chunk Nation.

(8) Posting non-business-related messages newsgroups. For purposes of this paragraph, a newsgroup is a repository for messages posted from many users at different locations and usually involves a discussion group.

10. **Service Access Guidelines**.

a. Each Nation governmental and enterprise entity office is routinely provided an e-mail address for access to the Nation's network.

b. Internet access is controlled by IT and users will be granted access unless IT, the user's Supervisor or the user's Executive Director determines that the user has violated this Act in the use of this access.

Penalties for violations of this Act will be handled pursuant to paragraphs 12 and 13 of this Act and the Employment Relations Act (6 HCC §5).

c. If Internet access has been previously denied or revoked, the Supervisor on the behalf of the user may petition IT for access upon the user's demonstration to the Supervisor that the user understands and acknowledges appropriate use of the Internet.

11. **Responsibilities**.

a. IT will provide necessary technology services for authorized users and assist Supervisors with the administration and monitoring of usage. Specifically, IT will:

(1) Provide access to technology service as required.

(2) Configure, monitor, and audit usage of each account and provide that information to the appropriate department managers as requested.

(3) Monitor network traffic to ensure minimal impact on normal work activities and make recommendations as needed.

(4) Restrict or prohibit access from Internet sites determined by management to be non-work related or in poor taste. Access to Internet sites must be related to work, official travel, or research.

b. <u>All Nation Branches of Government and Affiliated Entities</u>.

(1) Supervisors will submit a service request to IT for user access. The request will include the:

(a) Name of individual requiring access;

(b) Justification for requested access; and

(c) Any related information needed to provide proper access.

(2) Report changes to access lists as personnel changes occur.

(3) Ensure all users are aware of the provisions of this Act.

(4) Monitor technology usage and enforce the provisions of this Act.

c. <u>Users</u>.

(1) Each user is responsible for the proper usage of their technology services in accordance with this Act.

(2) The capability to write to removable media will be disabled by default. Write

access will be approved on a case-by-case basis. An appropriate request for access must be made with documented approval by the user's department head or director. All requests must include business or job-related reasoning for such access. IT will periodically review all approved access for current need and access may be adjusted with notification to the user's department head if the original justification no longer applies.

12. **Supervisor Action Upon Alleged Violation of this Act**.

a. When a violation of this Act is suspected by IT or the user's Supervisor there will be immediate notification to IT, the user's Supervisor, or the user's Executive Director, respectively. At the discretion of IT, the Department of Personnel will be notified without notification to the user's supervisor or Department.

b. IT and the Supervisor or Personnel will actively investigate each misuse of technology resources by an individual user. The investigation will attempt to determine the duration of the violation(s) and it will attempt to determine if the violation was intentional.

13. **Violations and Penalties**.

a. Except as provided in paragraph b. below, it will be the decision of the user's Supervisor, or the user's Executive Director with notification to the Department of Personnel and IT, if access will be terminated for a user's violation(s) of this Act. In addition to terminating access, the Supervisor may institute disciplinary action against an employee pursuant to the Nation's Employee Relations Act (6 HCC Sec. 5).

b. If it is obvious that a user has intentionally, frequently, and excessively misused technology resources, IT will deny or restrict all use of the abused service(s) immediately. Only in these cases may IT revoke all the abused privileges without advanced notice to the user's Supervisor or the user. If IT takes this action and at the determination of the user's Supervisor it is necessary for the user to have the use of abused service(s) to accomplish the user's job, the user may be disciplined up to and including termination.

c. In addition to the penalties provided in paragraph a. and b. above, the intentional misuse or abuse of Tribal property, including technology resources and services, may result in the denial of the service, imposition of cost for the personal use of the service, reimbursement to the Nation of wages paid to user while the user was misusing the resources and services, and disciplinary action up to and including termination.

d. Any violation of this Act may also result in litigation by the Nation to seek restitution from the user for intentional abuse and misuse of tribal property.

14. **Sovereign Immunity**.

a. Nothing in this Act will be deemed to waive the sovereign immunity of the Ho-Chunk Nation or any of its enterprises, officers, agents, or employees.

Legislative History:

4/04/00	Enacted by Legislative Resolution 4/11/00D.
10/25/01	Restated to conform paragraph numbering IAW format prescribed by the Legislative Organization Act of 2001.
8/10/06	The Act was referred to the Administration Committee to address the issue of using personal laptops in the workplace. The Computer Usage Act was sent out for comments. Motion to table Act for another month.
11/6/07	Motion to table Intranet/Internet Usage Act until next month for Legislative Attorney Report.
1/4/07	Legislative Attorney reviewed Act with MIS. A current draft of the Internet/Intranet Usage Act will be provided at the February 2007 Administration Meeting.
2/16/07	Motion to table Act for another 30 days to add language to ensure that Act prohibits use of personal laptops and change name of MIS to the Division of Information Technology (IT).
3/16/07	Motion to update Legislative History of the Computer Usage Act. Committee accepted changes made by Legislative Counsel to Act regarding prohibiting use of personal laptops and changing name of MIS to the Division of Information Technology (IT). Intranet/Internet Usage Act referred to full Legislature.
3/21/07	Final Draft was submitted to the Legislature who had no objections to the Final Draft and, pursuant to the Legislative Organization Act (2 HCC § 11), the Legislature placed the Final Draft out for forty-five (45) day comment on the Nation's Website.
05/10/07	Legislative Counsel provided the final draft to every Legislator and noted that during this forty-five (45) day comment period, the Legislative Counsel Office received no comments on the Final Draft.
05/22/07	Computer Usage Act enacted into law by Legislative Resolution 05/22/07B.
02/13/08	Special Counsel Michael Murphy presents proposed amendments to Administration Committee. Administration Committee motions to send proposed amendments to Legislature.
02/19/08	Legislature motions to send proposed amendments to the Office of the President.
04/29/08	Computer Usage Act amended and enacted into law by Legislative Resolution 04/29/08I.
3/26/09	IT Department provides recommended changes to the Legislative Counsel's Office to the Computer Usage Act to address security issues that have arisen since last time Act was amended by the Legislature.
04/07/09	Legislature passes motion to refer proposed Amendments to the Administration Committee.
05/07/09	The Administration Committee passes a motion to refer the amendments to the *Computer Usage Act* (6 HCC § 4) to the Legislature for further action.
05/19/09	Legislature passes Resolution 5-19-09 B placing proposed amendments to Computer Usage Act out for forty-five day public comment.
08/18/09	Legislature passes Resolution 8-18-09 B enacting proposed amendments to Computer Usage Act making the following substantive changes to Act: • Section 6 to provide examples of technological devices that are categorized as "personally owned computer equipment"; • Section 9, subparagraph b. (5) providing more expansive enumerated list of individuals who an employee cannot reveal his or her password. • Section 11, subparagraph c. (1) & (2) providing that the Nation's computers CD/DVD write capabilities will automatically be disabled by default, but that an employee with proper approval may have these functions enabled.
03/17/20	Legislature adopts Resolution 03-17-20 I quick passage of amendments to Section 6 of the Computer Usage Act to use personally owned equipment during an emergency.
01/18/22	Legislature adopts Resolution 01-18-22D enacting proposed amendments to Computer Usage Act now known as the Technology Resources Usage Act.