Policy:	#5-08
Approved By:	SLT
Approval Date:	February 12, 2020
Revision Date:	February 2025
Effective Date:	February 12, 2020
Date to be Reviewed:	February 2025
Administrator Responsible:	EVP Academic & COO

ACCEPTABLE USE OF INFORMATION TECHNOLOGY

POLICY STATEMENT

North Island College (NIC) provides information technology resources to support the educational and business activities of NIC. All members of the College Community must responsibly use and manage these resources. NIC will investigate allegations of misuse of information technology resources and apply disciplinary sanctions where appropriate.

PURPOSE STATEMENT

The purpose of this policy is to:

1. guide users in the acceptable use and management of NIC information technology resources; and
2. set out the rights and responsibilities of NIC and of the College Community in their use and stewardship of information technology resources.

DEFINITIONS

College Community members include:

1. all employees of NIC, whether employed on a full-time or part-time basis;
2. registered NIC students, past and present;
3. contractors and third parties required by contract to comply with NIC policies and procedures;
4. members of the Board of Governors; and
5. all other Users granted access to Information Technology Resources.

Information Security Incident means any adverse event whereby some aspect of information security could be threatened, including but not limited to loss of data or records confidentiality, disruption of data or system integrity, or disruption or denial of availability.

Information Technology Resources means equipment, systems, and infrastructure owned by, or in the custody or control of, NIC, including but not limited to:

1. computers;
2. laptops;
3. tablets;
4. smartphones;
5. servers;
6. data storage devices;
7. data;
8. records;
9. software;
10. telephones;
11. fax machines;
12. network services; and
13. electronic communication systems.

NIC Email Account means an email account provided by NIC to an employee, student, contractor, emeritus designate, or other User approved by the Director, Information Technology – Infrastructure & Educational Technologies.

Personal Data means any records or data relating to incidental personal use of Information Technology Resources, including but not limited to personal emails, documents, voicemails, text messages, and records of internet and social media use.

User means any individual, group, or organization that uses or accesses Information Technology Resources.

SCOPE AND APPLICATION

1. This policy is applicable to all Users and all members of the College Community, as well as to all Information Technology Resources, regardless of physical location.

2. NIC will investigate suspected violations of this policy in accordance with other NIC policies, collective agreements, terms of employment, and other contracts or agreements with third parties.

POLICY

Acceptable Use of Information Technology Resources

1. NIC provides Information Technology Resources to the College Community primarily to serve the education, research, and administrative purposes of NIC.

2. Any User of Information Technology Resources has primary responsibility for their use of them, and for any data or information they transmit, receive, use, or store through them.

3. Users are expected to respect the rights and property of others, including rights to privacy, to confidentiality, and over intellectual property.

4. Information Technology Resources may only be used in a manner that is consistent with:
   a. this policy and other NIC policies, including but not limited to:
      i. 1-01 Freedom of Information and Protection of Privacy;
      ii. 1-05 Records Management;
      iii. 1-20 Code of Ethical Conduct;
      iv. 2-08 Human Rights;
      v. 3-06 Community Code of Academic, Personal and Professional Conduct (Code of Conduct);
      vi. 3-27 Integrity in Research and Scholarship; and
      vii. 3-34 Sexual Violence and Misconduct.
   b. collective agreements;
   c. terms of employment applicable to non-unionized employees;
   d. other contracts or agreements with third parties; and
   e. applicable laws, including but not limited to the Canadian *Criminal Code*, the Canadian *Copyright Act*, the BC *Civil Rights Protection Act*, the BC *Human Rights Code*, and the BC *Freedom of Information and Protection of Privacy Act* and *Regulation.*

5. Prohibited uses of Information Technology Resources are any uses that disrupt or interfere with the use of the resources for their intended purpose. Examples of prohibited uses include but are not limited to:
   a. Seeking, without authorization, information on passwords or data belonging to another user;
   b. Making unauthorized copies of proprietary software, or offering unauthorized copies of proprietary software to others;
   c. Viewing, storing, or distributing sexually explicit or pornographic materials without legitimate academic purpose;
   d. Copying another person’s files, or programs, or examining such information unless authorized
   e. Using Information Technology Resources for commercial purposes without authorization, such as promoting by broadcast non-educational profit-driven products or services;
   f. Intercepting or examining the content of messages, files, or communications in transit on a voice or data network without authorization;
   g. Interfering with the work of other users of a network or with their host systems, disrupting the network, or engaging in any uses that result in the loss of another user's files or system;
   h. Creating or sending malicious or nuisance email, including spam or chain mail;

i. Sending communications (messages, images, etc.) that would be considered harassing or discriminatory per College policy or other legislation

j. breaching NIC policies or applicable laws;

k. misrepresenting the User's identity;

l. infringing upon the intellectual property protections of any works, data, computer programs, marks, names, or other representations serving to distinguish the goods or services of one person from another;

m. failing to maintain the confidentiality of passwords, access codes, or identification numbers used to access Information Technology Resources;

n. destroying, altering, dismantling, disfiguring, or disabling Information Technology Resources;

o. attempting to circumvent security controls on Information Technology Resources without authorization;

p. knowingly introducing a worm, malware or virus to Information Technology Resources; or

q. engaging in any uses that result in the loss of another User's information without authorization.

6. Nothing in paragraph 5 shall be construed as preventing or restricting duly authorized NIC staff from carrying out their duties.

Privacy of Users

7. An email or other record created using Information Technology Resources may be a college record for the purposes of the BC *Freedom of Information and Protection of Privacy Act.*

8. Incidental use of Information Technology Resources for personal use is not encouraged and should be limited to responsible activities that minimize the disruption of NIC business while attending to necessary personal affairs. NIC is not responsible for any Personal Data stored on Information Technology Resources:

   a. NIC takes reasonable measures to back up data and protect it from loss, but NIC cannot guarantee that Personal Data will be retained in NIC systems or remain confidential. Users are encouraged to store Personal Data separately from Information Technology Resources and back it up regularly to protect that personal data from inadvertent access, disclosure, or destruction. When Users store Personal Data on or intermingle it with Information Technology Resources, they increase the risk that NIC will unintentionally access that Personal Data while using Information Technology Resources for NIC business purposes.

   b. NIC routinely monitors network patterns such as source/destination, address/port, flags, packet size, packet rate, and other indicia of traffic on Information Technology Resources. NIC staff also perform routine maintenance (e.g. looking for malicious software, indications that unauthorized access to data has occurred or is occurring)

of Information Technology Resources, and that routine monitoring and maintenance may unintentionally reveal Personal Data.

c. In the event of an Information Security Incident or suspected contravention of this policy, NIC may temporarily expand the scope of routine monitoring activities to include computers, servers, and devices connected to the NIC network.

d. Electronic information does not necessarily disappear after it has been deleted. NIC may, in accordance with this policy, retrieve or reconstruct Personal Data generated, stored, or maintained on NIC systems even after they have been deleted.

9. NIC will not intentionally access, use or disclose Personal Data unless it has consent from the User, or:
   a. securing the User's consent would compromise
      i. the health or safety of an individual or group of people;
      ii. the availability or accuracy of the information; or
      iii. an investigation or a proceeding related to a breach of law, policy, collective agreement, or terms of employment of the User.
   b. a decision is made by the responsible authority in relation to
      i. Student information - Registrar;
      ii. Financial and Payroll information - Vice President, Finance;
      iii. Human Resources - Director, Human Resources.
   c. NIC is legally authorized to do so.

10. Notwithstanding paragraph 9, NIC will take such actions as are necessary to comply with any legal obligations.

Email Accounts

11. NIC Email Accounts will be managed and used in accordance with the NIC Email Procedures (Appendix A).

Compliance

12. Use of Information Technology Resources acknowledges acceptance of and compliance with this policy.

13. Users who breach this policy may be subject to a full range of NIC disciplinary actions including suspension or termination of employment. Violation of the policy may result in Information Technology Resource access restrictions or a permanent ban.

Collective Agreement References:

NIC/CUPE 3479 Collective Agreement
NIC/NICFA Collective Agreement and Common Agreement

Links to Other Related Policies, Documents and Websites:

Cellular Telephones #6-05
Code of Ethical Conduct #1-20
Community Code of Academic, Personal and Professional Conduct (Code of Conduct) #3-06
Freedom of Information and Protection of Privacy #1-01
Human Rights #2-08
Integrity in Research and Scholarship #3-27
Intellectual Property #3-28
Progressive Discipline Misconduct or Inappropriate Behaviour #2-12
Records Management #1-05
Sexual Violence and Misconduct #3-34

APPENDIX A
EMAIL PROCEDURES

EMAIL ACTIVATION/DEACTIVATION

1. NIC Email Accounts will be provided through the following processes:

    a. Students will receive NIC Email Accounts through the admissions process;

    b. Employees and contractors will receive NIC Email Accounts through the hiring process;

    c. Emeritus Designates will receive NIC email accounts on designation; and

    d. Exceptions to the above approved user groups must be approved by the responsible administrator within IT.

2. NIC Email Accounts for employees and contractors will be deactivated during off-boarding as follows:

    a. The employee's or contractor's supervisor will submit an action request to Human Resources indicating the departing employee's or contractor's email address, last day of work, and whether the supervisor requires access to the contents of the mailbox after the employee's departure; and

    b. IT will disable the employee or contractor's NIC Email Account within one (1) day after the employee's last day of employment or the final day of the contractor's contract.

EMAIL SECURITY/MONITORING

Users should not consider electronic communications private or secure and should be aware that all such records are College records that may be monitored and subject to disclosure under the Freedom of Information and Protection of Privacy Act.

CATEGORIES OF MONITORING

If there is an operational or managerial requirement to access or monitor an employee's email account, one of the following categories should be determined:

1. Non-Human Resources Related

a. **Administrative Access** – includes access to email, calendars and tasks to perform duties required of a position; and

b. **Extended Leaves** – access to email while employee is on leave to ensure continued workflow.

2. <u>Human Resources Related</u>

a. Human Resources related issues for the purpose of investigation, fact-finding or emergency access.

EMAIL ACCESS APPROVAL

1. The request must be approved by the Manager/Director of Human Resources prior to initiating. The following steps will be taken:

   a. Human Resources reviews the request with the requesting supervisor; final approval for monitoring will be in consultation and agreement with the responsible SLT administrator; and

   b. The monitored party may or may not be notified – issue specific.

2. The following process steps will apply to all requests:

a. Supervisor completes and submits the Email Access Request Form (attached) to the Manager/Director of Human Resources for review/approval;

b. Manager/Director of Human Resources reviews and approves the Email Access Request Form and obtains secondary approval from the responsible SLT administrator;

c. Human Resources provides the Email Access Request Form to the responsible administrator in IT for action;

d. The supervisor will advise the employee/contractor for all non human resources related monitoring periods;

e. Monitoring is initiated by IT based the approved start date; and

f. Monitoring is removed by IT on the approved end date or at the request of the original requesting supervisor, responsible SLT administrator or Manager/Director Human Resources

EMAIL ACCESS REQUEST FORM

This form is to be used if there is an operational or managerial requirement to access or monitor an employee's email account for a non-human resources related or Human Resources related reason. Complete this form and forward to the Manager/Director of Human Resources. Refer to Appendix A of NIC Policy #5-08 Acceptable Use of Information Technology at NIC.

Employee Name _____ **Employee ID#** _____

Start Date _____ **End Date** _____

Reason:

Access Request Type

Non-Human Resources Related

☐ Administrative Access - includes access to email, calendars and tasks to perform duties required of a position.

☐ Extended Leaves - access to email while employee is on leave to ensure continued workflow.

Human Resources Related

☐ Human Resources related issues for the purpose of investigation, fact-finding or emergency access.

Signatures

Supervisor:

Name _____ Signature _____ Date _____

Manager/Director Human Resources:

Name _____ Signature _____ Date _____

SLT Administrator:

Name _____ Signature _____ Date _____

IT Actions - Completed by:

Name _____ Signature _____ Date _____