

## **Procedure Title: Electronic Mail (Email)**

**Impact:** Employees, Students, Affiliates

**Responsibility:** Chief Information Officer

**Effective Date:** 4/18/2012

**Revised Date:** 5/11/2017

**Reviewed Date:**

**Relates to Policy(s):** 3.08.02

**Legal Citation(s):**

---

This procedure should be read in conjunction with the Electronic Mail and Acceptable Use Policies

### **I. Ownership and Access**

- A. NIC electronic mail (email) systems are the property of NIC and users of NIC email are subject to applicable NIC policies, Federal, and State laws.
- B. Users have a reasonable expectation of privacy in anything they create, store, send, or receive via email on NIC data and IT resources, yet NIC reserves the right to monitor email and the use of those resources for operational needs and to ensure compliance with applicable laws and NIC policies and procedures.
- C. When NIC receives a public records request, subpoena, litigation or other similar request for information or documents contained within the email system, NIC will take necessary measures to access these resources to comply with its legal obligations.

### **II. Assignment of Electronic Mail**

- A. Official NIC email accounts are available for all students enrolled in credit bearing courses. Employees will receive an official NIC email account during their employment at NIC. NIC Affiliates are assigned an email account as appropriate in relationship to their role with NIC.
- B. Termination of accounts is at the discretion of NIC. Guidelines are established by Information Technology (IT) in conjunction with the IT Policy and Planning Council (ITPPC), and available through the NIC IT Department.

### **III. Responsibility of Users**

- A. Users of NIC email must adhere to all applicable NIC policies, procedures, guidelines, contracts, and licenses as well all applicable federal, state, and local laws and regulations.
- B. Users of NIC email are expected to check their email on a frequent and consistent basis in order to stay current with NIC-related communications. Users have the responsibility to recognize that certain communications may be time-critical.
- C. Users are responsible for reporting violations of email use to the appropriate manager, administrator, or IT department.
- D. Incidental personal use of electronic mail is permitted; however, users are advised they have no guarantee of privacy or confidentiality in connection with the personal use of these resources.

Personal use must not:

- 1. Consume resources that interfere with normal NIC operations.
- 2. Interfere with work- and job-related duties.
- 3. Preempt any business activity.
- 4. Violate any NIC policy or applicable laws.

#### **IV. Acceptable Use**

The following items include guiding principles for acceptable use of email resources at NIC. The IT department in conjunction with the ITPPC will publish detailed guidelines and examples of acceptable and prohibited use cases.

##### **A. Guiding Principles**

- 1. Users will use NIC provided email in a lawful and appropriate manner.
- 2. Users will respect the integrity and the security of NIC email systems and data.
- 3. Users will be considerate of the needs of other users by making every reasonable attempt not to impede the ability of others to use email resources and show restraint in the consumption of email resources.
- 4. Users will respect the rights and property of others, including privacy, confidentiality, and intellectual property.
- 5. Users will cooperate with NIC to investigate potential unauthorized and/or illegal use of NIC email resources.

#### **V. Administration of Electronic Mail System**

The NIC IT department shall maintain and manage the email system used by NIC. IT and ITPPC will publish guidelines pertaining to the administration of the system to include, but is not limited to, distribution list creation, access to email accounts, account provisioning, aliases, name changes, and other related items.

## **VI. Privacy**

Users should use extreme caution in using email to communicate confidential or sensitive matters, and should not assume that email is private and confidential. It is important that users are careful to send messages only to the intended recipient(s). Particular care should be taken when using “reply” or “reply all” during email correspondence.

## **VII. Enforcement**

Regarding employees and other affiliates, the consequences of policy violation will be commensurate with the severity and frequency of the offense and may include termination of employment or contract.

Regarding students, the consequences of policy violations will be commensurate with the severity and frequency of the offense and may include suspension or expulsion.

Violations of this policy will be addressed in accordance with appropriate NIC policies and procedures, as issued and enforced by the appropriate authorities.

Violations of any local, state, or federal law will be reported to law enforcement.

Consequences of policy violation may include, but are not necessarily limited to, the following:

- A. Notification: alerting a user to what appears to be an inadvertent violation of this policy in order to educate the user to avoid subsequent violations.
- B. Warning: alerting a user to the violation, with the understanding that any additional violation will result in a greater penalty.
- C. Loss of computer and/or network privileges: limitation or removal of computer and/or network privileges, either permanently or for a specified period of time.
- D. Penalties: if applicable, the violator may be subject to criminal or civil penalties.

## **VIII. Appeal**

For employees, appeal of actions taken which result in an unresolved dispute will be handled via the Grievance Policy and Procedure. For students, all provisions of the Student Code of Conduct shall apply.

## **IX. Maintenance**

This procedure will be reviewed by NIC's Chief Information Officer (CIO), IT Department, and the ITPPC every three years or as deemed appropriate based on changes in technology or regulatory requirements.

## **X. Exceptions**

Exceptions to this procedure must be approved by the NIC IT Department and formally documented under the guidance of the CIO, and President's Cabinet.