State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

AMENDMENTS TO NITC 8-101

A. NITC 8-101 (Information Security Policy) is amended as follows:

1. Section 4.6 is amended to read:

4.6 ~~Asset~~ Data Classification

Data is a critical asset of the State of Nebraska. All staff have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the State of Nebraska, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).

Agencies are responsible for establishing and implementing appropriate managerial, operational, physical, and technical controls for access to, use of, handling of, transmission of, and disposal of State data in compliance with this policy and the agency Records Retention schedule. The agency data owner should carefully evaluate and determine the appropriate data sensitivity or classification category for their information. Assigning classifications determines day-to-day practices with information: how it is handled, who handles it, how it is transported, stored, who has access, where it can go, etc.

Data owned, used, created or maintained by the State is classified into the following four categories:

- ~~Public~~
- ~~Internal Use Only~~
- ~~Confidential~~
- ~~Highly Restricted~~

~~(See NITC Security Officer Handbook)~~

- Highly Restricted. This classification level is for the most sensitive information intended strictly for use within your organization and controlled by special rules to specific personnel. Examples of this type of data include Federal Tax Information (FTI), Patient Medical Records covered by Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) information, and any other information regulated by State or Federal regulations. This level requires the greatest security protection and would have a high impact in the event of an unauthorized data disclosure.

- Confidential. This classification level is for sensitive information that may include Personally Identifiable Information (PII) intended for use within your organization. This level requires a high level of security and would have a considerable impact in the event of an unauthorized data disclosure.

- Managed Access Public. This classification level is for information that is public in nature but may require authorization to receive it. This type of information requires a minimal level of security and would not have a significant impact in the event of data disclosure. This type of information does not include personal information but may carry special regulations related to its use or dissemination. Managed Access Public data may also be data that is sold as a product or service requiring users to subscribe to this service.

- Public. This classification is for information that requires no security and can be handled in the public domain.

2. Section 4.8.2.1 is amended to read:

4.8.2.1 Security of Electronic Mail

Electronic mail provides an expedient method of creating and distributing messages both within the organization and outside of the organization. Users of the state E-mail system are a visible representative of the state and must use the system in a legal, professional and responsible manner. ~~Users must comply with this policy, the Records Management Act, and be knowledgeable of their responsibilities as defined in NITC Secure E-Mail for State Agencies.~~ An account holder, user, or administrator of the State email system must not setup rules, or use any other methodology, to automatically forward all emails to a personal or other account outside of the State of Nebraska network.

B. All NITC Standards and Guidelines which reference data classification categories modified in Section A.1 of this Amendment are amended accordingly.