### Tier 1 Control Standards (State-Wide)

**Electronic Mail**

**Standard ID**  
IOT-CS-SEC-115

**Published Date**  
3/1/2008

**Effective Date**  
3/1/2008

**Last Updated**  
5/17/2017

**Next Review Date**  
5/17/2018

**Policy**  
11.0 Protective Technology (PR.PT)  
11.4 PR.PT-4  
11.4.1 Network Protection

**Purpose**  
IOT provides email services to support the administrative functions of the State. Employees must be mindful that email is a business tool and it shall be used as such. Employees shall never use email to send any message that would be a source of embarrassment to the sender, to the recipient, or to State if the message were to be seen by others. Electronic mail is a public record.

**Scope**  
IOT Supported Entities

**Statement**  
All email and attachments transmitted or received over the State Network are subject to the provisions of this Standard. Additionally, as Indiana Law provides that email communications written in the conduct of public business are generally considered to be public records, all email communications written and sent in the conduct of public business by the State workforce are subject to applicable provisions of this Standard regardless of the device (public or privately owned) used to send or receive the communication.

**General**

Workforce members shall review and abide by the appropriate use guidelines covered in the Information Resources Use Agreement (IRUA). Agency de minimis guidelines apply when email use is for non-business purposes. Caution should be applied when sharing jokes, pictures, or potentially controversial subjects. Differing perspectives can result in an email being deemed inappropriate by recipients or management.

When sending messages, workforce members must be cognizant of both the message size and number of individuals in the distribution list. Emailing sizeable files to large numbers of people can slow the State’s email system. Such circumstances can result in disciplinary action.

Workforce members, especially in situations when erroneously addressed on an email, are discouraged from use of the “reply all” function. There is no need to compound another’s mistake by “replying to all”. I may harm email performance. Again, such circumstances can result in disciplinary action.
Prohibited Email Practices

The following activities are expressly prohibited:

1. Sending obscene or patently offensive email;
2. Sending intimidating, threatening, harassing, or abusive email;
3. Clicking on links in spam messages;
4. Clicking on attachments containing malware;
5. Interception, disrupting, or altering an email communication without proper authorization;
6. Accessing, copying, or modifying email messages from or within the electronic files or records of another without permission;
7. Misrepresenting the identity of the source of an email communication;
8. Allowing another to use one's email account for fraudulent purposes;
9. Using email to interfere with the ability of others to conduct state business;
10. Sending unsolicited "junk" email or mass electronic mailings, such as chain letters, without a legitimate business purpose;
11. Using email for commercial purposes unrelated to state business;
12. Using email for prohibited political activities as described under State Ethics Code.
13. Reproducing or distributing copyrighted materials without appropriate authorization; and
14. Using email for any purpose which violates state law, federal law, or state policy.

Application of Public Records Statutes to Email

Email messages are subject to many of the same statutes and legal requirements as other forms of communication (e.g. - the Indiana Public Records Act, Indiana Code 5-14-3 governing public access to State records). The Public Records Act treats electronic documents and files in the same manner as paper documents. All such documents are generally considered to be public records and are subject to public inspection unless they are covered by a specific statutory exception. Email messages which are public records must be retained in either paper or electronic format. Email messages which are not public records should be deleted after viewing. State record retention policy requires that all documents pertaining to the business of the State whether in paper or electronic form, be retained, archived, or destroyed, as appropriate. Disposition decisions regarding individual documents should be made in accordance with the State general record retention policy and agency record retention policy with guidance provided by the agency records coordinator and Indiana Commission on Public Records. Although current IOT practice includes the back-up of email, such back-up is only undertaken for recovery purposes and is not intended to serve as a mechanism for archiving public records.

Privacy and Confidentiality

State email messages should never be considered private communications. Confidentiality of email cannot be guaranteed by the State for many reasons including the following:

- Public records statutes,
- Email messages may be saved indefinitely on the receiving computer,
- Copies of email messages can be made electronically or on paper,
- Email messages can be intentionally or accidentally forwarded to others,
- And messages may be sent to incorrect email addresses or be improperly delivered by an email system.

Monitoring of Email Communications

IOT does not monitor email usage in a regular or systematic fashion. However, it does reserve the right to monitor usage as a means of troubleshooting or standard maintenance activities. IOT will also provide information on email activities when requested to do so by authorized agency contacts. Such monitoring may include tracking addresses of email sent and received, accessing in-box messages, accessing messages in folders, and accessing archived messages in accordance with the Workforce Computer Activity Review and Restore Standard. Individual Agencies may take corrective action or disciplinary action based upon information obtained from a review of his or her email communications. Disciplinary actions are not determined by IOT. Furthermore, IOT may disclose email communications sent to, received by, or relating to an employee on a request by law enforcement officials. Prior notice will not be provided to employees on any of the circumstances discussed above.
Roles
Agency Management
All Personnel
IOT Personnel

Responsibilities
All Personnel shall abide by this Standard and report inappropriate use of email or SPAM. Agencies shall develop and communicate internal policies regarding email use and record retention. IOT shall support email and email storage.

Management Commitment
Management is responsible for ensuring their agency is meeting the requirements written within this Standard.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT where necessary and with the appropriate staff to meet the requirements written within this Standard.

Compliance
IOT will not actively monitor end user email activities but will work with agencies when requested to provide personal information. Individuals found to have violated this Standard may be subject to disciplinary actions up to and including termination of employment.

Exceptions
No exceptions.