



S T A T E O F M A R Y L A N D
DEPARTMENT OF INFORMATION TECHNOLOGY

E-Mail Encryption Policy

1.0 Introduction

The State has requirements to retain, protect, and recover data within its stewardship, and has established policies and practices to meet these obligations. Employees and contractors of the State, in the course of business, may send or receive confidential information using via email. Exchange of confidential information and official correspondences must be done in a way that is secure and protects citizen data.

The purpose of this policy is to define acceptable guidelines for sending e-mail containing confidential information. Any employee who uses email to send confidential information shall use an appropriate encryption service. Agencies have been provided access to licenses that encrypt messages sent by Google Apps to addresses outside the Maryland.gov domain. Agencies using other email systems must independently procure a solution to encrypt email sent to an address external to that system.

2.0 Scope

This policy shall apply to all employees and contractors assigned an email account on a State e-mail system.

3.0 Policy

3.1 General

1. Employees and contractors shall obtain an encryption license if they have a business need that requires sending confidential data by email to an email address that is external to the email system. Employees and contractors utilizing the Maryland.gov email system shall obtain an encryption license for Google Mail provided by the Department of IT.
2. Employees and contractors shall not place confidential information in the "Subject" line of any email message.
3. Employees and contractors that receive confidential information from a citizen by email shall not reply to the message unless they utilize encryption or remove the confidential information from the reply message.
4. Employees and contractors that receive confidential information from a citizen by email that is listed in the "Subject" line of the message will redact the information from the "Subject" line prior to replying and use encryption as appropriate.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Deliberate, unauthorized disclosure of confidential information may result in civil and/or criminal penalties.