		Effective:	7/1/2017
		Last Review:	7/1/2017
Title:	Prohibited Use of Password Protected Content & Pre-Encrypted Attachments	Next Review:	Annually
Number:	ISP-195		
Version:	1.01	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

To ensure that text based documents, which are converted into an image format, are converted into an Optical Character Recognition (OCR) compatible format. To ensure that using local password protecting and pre-encrypting of content or attachments that impede discovery capabilities is prohibited; especially, SOA information asset content or attachments containing Personally Identifiable Information (PII), Electronic Protected Health Information (EPHI), Payment Card Industry Data Security Standards (PCI DSS), Criminal Justice Information Security (CJIS) or any other information protected by State, federal or local laws in electronic mail (email).

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to all SOA branches, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Local password protection and attachment encryption are prohibited;
- Image format text based documents must be converted to OCR; and
- SOA system wide encryption must be implemented.

5.1. Prohibit Local Password Protection and Attachment Encryption

5.1.1 Prohibit Local Password Protection & Attachment Encryption

It is the SOA's fiduciary responsibility to monitor email systems for internal policy compliance, suspected criminal activity, privacy of personally identifiable information (PII) and other systems management reasons. Using local password protecting and pre-encrypting of content or attachments that will impede discovery capabilities is prohibited. SOA is required to meet authorized public records requests, comply with State, federal and local statutes, regulations and policies and retain the ability to appropriately store and process SOA government documents and records.

5.2. Ensure All Image Format Text Based Documents are Converted to OCR and Encrypted

5.2.1 Ensure All Image Format Text Based Documents are converted to OCR compatible format

It is the SOA's responsibility to ensure that all text based documents (e.g., birth certificate) that have been changed to an image format are converted into an OCR compatible format for attachment.

5.2.2 Ensure Encryption

SOA emails, outbound to external domains, containing PII, EPHI, PCI DSS or CJIS information must be encrypted, as defined in SOA policy ISP-194 External Email Encryption.