Title	**E-mail encryption policy**
Type	Policy
Category	Security
Status	Approved
Approved	01/09/2013
Revised	12/21/2012
Scope	Defines acceptable uses for Public Key Infrastructure relating to City e-mail services. Applies to all City e-mail use in conjunction with said infrastructure.
Policy	**Policy Definitions:** • Certificate Authority: an individual or agency trusted and empowered to create and sign certificates. • Ciphertext: data that has been encrypted. Ciphertext is unreadable until it has been converted into plaintext ("decrypted") with a key. • Credentials: a user's keypair and associated passphrase. • Encryption Algorithm: a mathematical procedure for performing encryption on data. Through the use of an algorithm, information is made into meaningless ciphertext and requires the use of credentials to transform the data back into its original form. • Decryption: the process of decoding data that has been encrypted into a secret format. Decryption requires a set of credentials. • Digital Certificate: an attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. • Digital Signature: an electronic analogue of a written signature in that the digital signature can be used in proving to the recipient or a third party that the message was in fact signed by the originator. • Encryption: the translation of data ("plaintext") into a secret code ("ciphertext"). To read an encrypted file, you must have access to the credentials that enable you to decrypt it. • Key Escrow: a data security measure in which a cryptographic key is entrusted to a third party (i.e., kept in escrow). Under normal circumstances, the key is not released to someone other than the sender or receiver without proper authorization. Key escrow is used to ensure that there is a backup of the cryptographic key in case the parties with access to keys lose the

data through a disaster or malicious intent.

- Keypair: a combination of a user's public and private encryption keys.
- Passphrase: a set of numbers, letters and special characters known only by the user of a keypair (similar in concept to a password) that guards the private key from misuse by others.
- Plaintext: textual data in human-readable ASCII format. Plaintext refers to any message that is not encrypted into or has been decrypted from ciphertext.
- Verification: the process of ensuring that a given digital signature is valid and positively identifies the originator of a message.

POLICY PROVISIONS

1. The Department of Technology and Innovation (DTI) shall establish a Certificate Authority for the purpose of issuing and maintaining credentials for users of its information technology assets related to encryption and digital signatures. DTI shall obtain Public Key Certificates for the Certificate Authority from one of the global Certificate Authorities.
2. When encrypting or digitally signing messages using the City's e-mail facilities, employees shall use only credentials issued by the City Certificate Authority. All credentials obtained by employees from third parties prior to the implementation of this policy and used to encrypt or sign City e-mail messages shall no longer be used and shall be surrendered to the Certificate Authority.
3. Credentials issued to an employee for encryption remain at all times the property of the City of Albuquerque. The City shall at all times have access to the employee's credentials (i.e., via escrow or alternate decryption key) for purposes of decryption and/or verification, and said credentials shall be immediately revoked upon the employee's retirement, termination, or transfer to another Department.
4. Approved encryption software titles, supported algorithms, minimum key lengths, etc., shall be published in one or more Standards.
5. Credential issuance and revocation processes shall be published in one or more Procedures.

ACCEPTABLE USES

Digital Signatures

- Encrypted e-mail messages **must be signed** under all circumstances.
- Plaintext e-mail messages sent by City to non-City e-mail users **may be signed**.
- Plaintext e-mail messages sent between City e-mail users only **may be signed**.
- E-mail messages not related to the official business of the City as defined by City policies **must not be signed** under any circumstances.

Encryption

City e-mail messages sent by City to non-City e-mail users **must be encrypted** if they contain:

- data defined in the sensitive data policy.
- data which reasonably qualifies for exemption from public disclosure under the New Mexico Inspection of Public Records Act;
- data barred from public disclosure by other Federal or State law or City ordinance;
- data barred from public disclosure under contract or pursuant to a court order.

City e-mail messages sent between City e-mail users only **must be encrypted** if they contain:

- data defined in the sensitive data policy
- data which reasonably qualifies for exemption from public disclosure under the New Mexico Inspection of Public Records Act;
- data barred from public disclosure by Federal or State law or City ordinance;
- data barred from public disclosure under contract or pursuant to a court order.

City e-mail messages sent by City e-mail users to any recipient **must not be encrypted** if they contain:

- data reasonably subject to inspection as public record pursuant to the New Mexico Inspection of Public Records Act;
- information of a personal nature and/or not related to the official

	business of the City.
Rationale	Enables a secure information sharing capability that provides for: • authentication -- proof that a message originator is who he/she claims to be (public/private key); • non-repudiation -- assurance that the message originator cannot later deny participation (digital signature); • integrity -- verification that no unauthorized modification of data has occurred (hash); • confidentiality -- assurance that the person receiving the message is the intended recipient (encryption/decryption). See also: • Health Insurance Portability and Accountability Act (Public Law 104-191, 110 Stat. 1998 [1996]; 42 USC 1301 et seq). • New Mexico Inspection of Public Records Act (14-2-1 et seq NMSA 1978). The City Legal Department can address Departments' questions concerning these statutes.