WELDO
Rebuilding Lives

Encryption Policy

1 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.

2 Scope

This policy applies to all WELDO employees and affiliates.

3 Policy

3.1 Proven, standard algorithms such as DES, 3DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. WELDO's key length requirements will be reviewed annually and upgraded as technology allows.

3.2 All Mobile devices (including Laptops, tablets PCs, Mobile Phones, USB drives, removeable media etc.) carrying sensitive data should be encrypted.

3.3 All network communication outside of the WELDO office premises should also be encrypted.

3.4 All email communication should be encrypted with TLS or SSL.

3.5 The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by DPO.

4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

5 Definitions

Term:	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).