Acceptable Encryption Standard

1.1 Overview

To protect sensitive information from exposure in the event of media or computer theft, information in all forms must be encrypted to ensure its confidentiality and security and prevent deliberate and accidental unauthorized disclosure.

To ensure that CPAC's information assets remains secured appropriately, effective encryption controls are defined in this document. CPAC may impose more stringent direction at its discretion.

1.2 Purpose

The purpose of this document is to provide a set of minimum encryption standards (hereinafter called 'the Standard') to be implemented in the context of CPAC's information assets.

This Standard will provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.

1.3 Scope

This standard is mandatory and applies to all CPAC employees, consultants and contractors who supply, install, procure or enable the use of encryption technologies.

1.4 Standards

i. Only proven, standard algorithms such as AES, Blowfish, RSA, RC5 and IDEA may be used as the basis for encryption technologies. Commercial or 'shareware' implementations of these algorithms may be used. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA -Hellman, while Secure Socket Layer (SSL) uses RSA encryption.

ii. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. CPAC's key length requirements will be reviewed annually and upgraded as technology allows.

iii. The use of proprietary encryption algorithms is not permitted, unless explicitly reviewed by qualified third party experts, and approved by CPAC's Information Technology Director. Note that encryption technologies are regulated by both Canadian and International law.

1.5 Enforcement

Failure to comply with this standard may result in actions by CPAC which include but are not limited to the following:

i. Denial of access to CPAC's information assets and information technology assets.
ii. Contractual remedies, as may be appropriate for third party suppliers, consultants and/or contractors, such as provisions for breach or termination of contract.
iii. Disciplinary action for employees, including, but not limited to, written warnings, suspensions with or without pay, and/or immediate termination of employment; and/or Prosecution under law.

1.6 Definitions

Term	Definition
Information assets and Information Technology Assets	Computer equipment (including laptop and desktop computers), software, operating systems, storage media, network accounts, electronic mail, internet access, portals, gateways, network devices, mobile devices, servers, telephones and telephone systems, multifunction printers, personal/home computers while they are connected to the CPAC network either directly or over a VPN connection, information assets (whatever the media or format type) such as business or personal information, and any other thing that may be considered by CPAC to be an information and information technology asset.
AES	Advanced Encryption Standard (AES) is a symmetric-key encryption standard heavily used within the Canadian Federal and Provincial Governments and healthcare providers throughout Canada. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael.

Blowfish	Blowfish is a keyed, symmetric block cipher and provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. It has since been superseded by the more readily adopted Advanced Encryption Standard.
RSA	Rivest, Shamir and Adleman (RSA) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption.
RC5	RC5 is a block cipher notable for its simplicity. Designed by Ronald Rivest, it was the foundation for the development of the Advanced Encryption Standard (AES) also known as RC6.
IDEA	International Data Encryption Algorithm (IDEA) is a block cipher and is a block cipher that is also symmetric. The algorithm was intended as a replacement for the Data Encryption Standard, however; AES was more widely adopted as a DES replacement.

1.7 Related Documents

- Information Management Policy
- Protection of Personal Information Policy
- Information and Information Technology (I&IT) Security Policy
- IT Infrastructure Security Standard

End of Document