Besseggen Cryptographic Control Policy

Doc: Version: 2.0

Document Classification: Internal

Document Control

Document Name	Besseggen Cryptographic Control Policy
Abstract	This document describes the Cryptographic Control policy at Besseggen Infotech LLP.
Security Classification	Internal
Location	SECTOR-94, NOIDA, GAUTAM BUDH NAGAR-201301

Authorization		
Document Owner	Reviewed by	Authorised by
IT Team	Head – IT	Head – IT

Amendment Log				
Version	Modification Date	Section	A/M/D	Brief description of change
1.1	15 Apr 2022	All	A	Final
1.2	1 May 2022	6	M	Reviewed

Distribution list
Chief Information Security Officer (CISO)

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

Auditors (Internal & External)
All users, committee at Besseggen Infotech LLP.

TABLE OF CONTENTS

1. Purpose

This policy defines the standards and controls that will be followed in order to maintain a minimum level of protection for information assets at Besseggen Infotech.

2. Scope

This policy applies to all employees, contractors, consultants, and temporary staff etc. who have access to Besseggen Infotech resources. All are expected to be familiar and comply with this policy.

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

3. Policy Statement

Information assets must be secured from unauthorized access, damage or interference. Cryptographic controls shall be implemented to ensure the confidentiality, authenticity or integrity of information assets located within Besseggen Infotech

4. Responsibility for Policy

The HEAD – IT is responsible for development, maintenance, implementation, operation and escalation of enforcement of these policies and standards.

5. Procedures

Encryption type and other implementation details shall be decided based on the relevant legislations and the level of protection required for the information. A regular review shall be carried out to determine the level of protection required by the information. This assessment shall be further used to determine the need of cryptographic controls, type of cryptographic control required.

Proven, standard algorithms such as 3DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for proven secure applications. 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 crypto-system key lengths shall be at least 128 bits. Asymmetric crypto-system keys shall be of a length that yields equivalent strength. Besseggen Infotech's key length requirements shall be reviewed annually and upgraded as technology allows.

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

The use of proprietary / closed encryption algorithms shall not be allowed for any purpose, unless reviewed by qualified experts independently of the vendor in question.

- The various needs for encryption of information involved in business transactions shall be derived from
  - Risk assessment
  - Customer requirement(s)
  - Regulation/Law/Standards compliance requirement(s)
- Based on business requirements, business sensitive and restricted / confidential data shall be stored and encrypted if necessary.
- A secure method shall be adopted for key management while using encryption methodologies in Besseggen Infotech.
- Passwords to access private keys, if any, shall be adequately protected from unauthorized intrusion.
- Any IT system utilizing encryption methodologies for protection of confidentiality of information shall be implemented based on approval from Head – IT.
- Depending on the business requirements, the information owner and IT shall decide a mutually acceptable encryption methodology for protecting identified critical and sensitive business information.
- Import, export and use of encryption methodologies shall be in compliance with applicable laws and regulations.
- Users possessing the private keys (in case of public key cryptographic methodologies) shall be responsible for safety of the keys during usage in the organization.
- Users shall be accountable and responsible for the transactions and safe maintenance of the private encryption keys assigned to them for usage.
- Usage of private encryption keys shall provide confidentiality, integrity, traceability and non - repudiation for the transactions involving identified critical applications.
- Specific procedures shall be adopted for private encryption key issuance, management, revocation and storage.

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

6. Good practices

6.1 Encryption

- Encryption is a cryptographic technique that can be used to protect the confidentiality of information. Appropriate levels of encryption shall be considered for the protection of sensitive or critical information.
- Besseggen Infotech should consider the use of cryptographic controls for protection of some of the information. The following should be implemented:
  - The use of at least 128-bit SSL certificates issued by a reliable and well known certification authority shall be used for securing browser to web server communications for Internet based transaction-oriented websites.
  - Appropriate levels of encryption of passwords for application, database, operating system and network devices.
  - Use of Hardware Security Modules (HSM) is highly advised as they are more secure than software enabled modules.
  - Use of PGP or similar asymmetric (public) key encryption for sharing the confidential data with the external parties via an email system

6.2 Non-Repudiation Services

Non-repudiation services should be used where it might be necessary to resolve disputes about occurrence or non-occurrence of an event or action, e.g. the use of a digital signature on an electronic contract or payment. They can help establish evidence to substantiate whether a particular event or action has taken place, e.g. denial of sending a digitally signed instruction using electronic mail. These services are based on the use of encryption and digital signature techniques.

6.3 Key Management

Protection of Cryptographic Keys

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

- The management of cryptographic keys is essential for the effective use of cryptographic techniques. Any compromise or loss of cryptographic keys may lead to a compromise of the confidentiality, authenticity and/or integrity of information. A management system should be in place to support the organization's use of the cryptographic techniques.
- All keys should be protected against modification and destruction, and Secret / Private keys need protection against unauthorized disclosure. Cryptographic techniques can also be used for this purpose.
- Physical protection should be used, to protect equipment used to generate, store and archive keys.

Standards, Procedures and Methods

- Key management also includes the technical, organizational and procedural aspects that are required to support the use of cryptography. The main objective of key management is the secure administration and management of cryptographic keys and related information. Key management includes the generation, registration, certification, de-registration, distribution, installation, storage, archiving, revocation, derivation and destruction of keys. Any compromise or loss of cryptographic keys could compromise the confidentiality, integrity or authenticity of information.
- A key management system should be based on an agreed set of standards, procedures and secure methods.
- In order to reduce the likelihood of compromise, keys should have defined activation and deactivation dates so they can only be used for a limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used and the perceived risk.
- Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information may need to be made available in an unencrypted form as evidence in a court case.
- The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

for the provision of services.

7. References

None

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)