Cryptography Policy

Policy Owner: Billy Caldwell

Effective Date: 06/27/2022

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information. This policy establishes requirements for the use and protection of cryptographic keys throughout their entire lifecycle.

Scope

This policy applies to all employees of Darwin Global or its divisions and its wholly-owned subsidiary and to all external parties with access to Darwin Global engineering data/information, information systems, networks, and system resources.

All information systems developed and/or controlled by Darwin Global LLC, its divisions and subsidiaries that store or transmit confidential data.

Policy

Darwin Global LLC shall evaluate the risks inherent in processing, and storing data, and shall implement cryptographic controls to mitigate those risks where deemed appropriate. Where encryption is in use, strong cryptography with associated key management processes and procedures shall be implemented and documented. All encryption shall be performed in accordance with industry standards, including NIST SP 800-57.

For all personal data, Darwin Global LLC shall consider the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons, and implement appropriate technical and organizational measures surrounding the pseudonymization and encryption of data to ensure a level of security appropriate to the risk.

For all web traffic sent over the public Internet containing confidential, the TLS v1.2 protocol or better must be utilized.

Key Management

Access to keys and secrets shall be tightly controlled in accordance with the Access Control Policy.

The following table includes the recommended usage for cryptographic keys:

Domain	Key Type	Algorithm	Key Length	Max Expiration
Web Certificate	Digital Signature	DSA or RSA PCKS#1	2048 bit	Up to 2 years for normal certificates, up to 10 years for root certificates.
Web Cipher	Encryption	AES	256 bit	N/A
Confidential	Encryption	AES	256 bit	1 Year
Password	Hash	Bcrypt, PBKDF2, or scrypt, ECDH	256 bit+10K Stretch	N/A
Laptop HDD	Encryption	AES	128 or 256 bit	N/A

Exceptions

Requests for an exception to this policy must be submitted to the Chief Software Architect, Information Systems Operations Manager, and the ISO for approval.

Violations & Enforcement

Any known violations of this policy are to be reported to any members of management or operations. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with the Darwin Global LLC Employee Handbook up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	06/27/2022	SOC2/2022	Diana Hussein	