Cryptography Policy

Greenrock Energy

Version 1.0 | 16 May 2026

1. Purpose

This policy defines the cryptographic standards and controls used by Greenrock Energy to protect data confidentiality, integrity, and authenticity across all systems, with particular focus on the Greenrock Energy CRM system and associated infrastructure.

2. Scope

This policy applies to:

- The Greenrock Energy CRM application (crm.greenrockenergy.co.uk)
- The hosted database server managed by Hosting Heroes
- The Head Office file server (WD My Cloud PR4100 NAS)
- All staff endpoint devices used to access company systems
- All data in transit between users and company systemsAll stored (at rest) data containing personal or business-sensitive information

3. Policy Statements

Greenrock Energy shall ensure that appropriate cryptographic controls are applied to protect data throughout its lifecycle. Only current, industry-recognised algorithms and protocols shall be used. Deprecated or known-vulnerable algorithms are prohibited.

11 Dunkirk Business Park, Frome Road, Southwick, Trowbridge, Wiltshire. BA14 9NL

Phone: 01225 753755

Email: info@greenrockenergy.co.uk

(GreenRock Energy is a trading name of Bennett Associates Consulting Limited).

4. Encryption in Transit

All data transmitted between users and company systems must be encrypted using Transport Layer Security (TLS) version 1.2 or higher.

4.1 Web Application (CRM)

- The CRM is served exclusively over HTTPS with TLS 1.2+ enforced.
- SSL/TLS certificates are provided via Let's Encrypt and are automatically renewed.
- TLS 1.0 and TLS 1.1 are disabled on the hosting server.
- All HTTP requests are redirected to HTTPS.

4.2 Head Office File Server (NAS)

- File access uses SMB 2 and SMB 3 protocols only. SMB 1 is disabled.
- NTLMv2 authentication is enforced; NTLMv1 is disabled.
- FTP, NFS, and SSH access are disabled.
- The NAS is accessible only on the local Head Office network; remote access is disabled.

5. Encryption at Rest

5.1 Hosted Database Server

The CRM database is hosted by Hosting Heroes in ISO 27001 and PCI-DSS accredited data centres. Full disk encryption (FDE) is in place at the hardware layer. All backups are encrypted by the hosting provider.

5.2 Application-Level Encryption

Sensitive fields within the CRM audit log are encrypted at the application level using AES-256-CBC with HMAC-SHA256 for integrity verification. Encryption keys are stored separately from the encrypted data.

5.3 Endpoint Devices

All staff endpoints must have full disk encryption enabled. Windows 11 devices must use Device Encryption or BitLocker, utilising the TPM 2.0 hardware security module. Staff are required to confirm that encryption is enabled on their devices.

5.4 Head Office File Server

The WD My Cloud PR4100 NAS does not support hardware encryption at rest. The following compensating controls are in place:

- Physical access to the NAS is restricted to authorised staff at Head Office.
- Network access is limited to the local LAN only; all remote access is disabled.
- Access to job files via the CRM is restricted by IP address to the Head Office network.
- User-level authentication is enforced on all NAS shares.

6. Password and Authentication Cryptography

6.1 Password Storage

User passwords are hashed using the bcrypt algorithm with a minimum cost factor of 10. Passwords are never stored in plain text or using reversible encryption. A minimum password length of 12 characters is enforced, requiring uppercase, lowercase, numeric, and special characters.

6.2 Multi-Factor Authentication (MFA)

MFA is mandatory for all users and uses Time-based One-Time Passwords (TOTP) as defined in RFC 6238. TOTP secrets are generated using cryptographically secure random number generation and codes are verified using HMAC-SHA1, the standard algorithm specified in the TOTP RFC. Recovery codes are hashed using bcrypt before storage.

7. Prohibited Algorithms and Protocols

The following algorithms and protocols are prohibited for use in any Greenrock Energy system:

Category	Prohibited
Encryption	DES, 3DES, RC4, Blowfish
Hashing	MD2, MD4, MD5, SHA-1 (for signing/certificates)
Protocols	SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1
Authentication	NTLMv1, LAN Manager (LM)
File Sharing	SMB 1.0/CIFS

Note: HMAC-SHA1 is permitted for TOTP authentication as specified in RFC 6238. This is distinct from the use of SHA-1 for digital signatures or certificate validation, which is prohibited.

8. Key Management

- Encryption keys must be stored separately from the data they protect.
- SSL/TLS certificate renewal is automated via Let's Encrypt.
- Application encryption keys are stored in a dedicated configuration file with restricted file permissions, outside the web-accessible directory.
- MFA secrets are stored in the database and are unique per user.
- Access to encryption keys is restricted to system administrators.
- Encryption keys must be changed if a compromise is suspected.

9. Network Security Controls

In addition to cryptographic controls, the following network security measures are in place:

- Imunify360 firewall and ModSecurity Web Application Firewall (WAF) on the hosted server.
- Enterprise-grade DDoS protection provided by the hosting provider.
- IP-based access restrictions for Head Office file access via the CRM.
- Single active session enforcement per user account.
- 30-minute session timeout for inactive sessions.

10. Compliance

This policy supports compliance with the UK General Data Protection Regulation (UK GDPR) Article 32, which requires appropriate technical measures to ensure the security of personal data processing, including encryption. It also supports the requirements of Legal & General's third-party information security assessment.

11. Policy Review

This policy shall be reviewed annually, or sooner if there are significant changes to the threat landscape, regulatory requirements, or company infrastructure. Reviews will assess whether current algorithms and key lengths remain appropriate and whether any prohibited algorithms have been inadvertently introduced.

Version	Date	Author	Changes
1.0	16 May 2026	Mark Brebner	Initial release

Name: Jason Lloyd Position: Director

Signature: *J Lloyd* Date: 18/05/2026

11 Dunkirk Business Park, Frome Road, Southwick, Trowbridge, Wiltshire. BA14 9NL

Phone: 01225 753755

Email: info@greenrockenergy.co.uk

(GreenRock Energy is a trading name of Bennett Associates Consulting Limited).