GREENROCK ENERGY

CRM System

TECHNICAL & ORGANISATIONAL SECURITY MEASURES

CONFIDENTIAL

Document Details	
Version	2.0
Date	16 May 2026
Classification	Confidential
Owner	Greenrock Energy
Last Audited	16 May 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).

1. Executive Summary

This document details the technical and organisational security measures implemented within the Greenrock Energy CRM system to protect personal data in accordance with Article 32 of the UK GDPR.

The CRM is a PHP-based web application hosted at crm.greenrockenergy.co.uk, using a MySQL database. It is accessed by staff and authorised contractors for managing energy assessment operations.

Security posture summary:

Security Area	Status	Risk Level
Password Hashing (bcrypt)	IMPLEMENTED	LOW
Password Complexity (12-char minimum)	IMPLEMENTED	LOW
Two-Factor Authentication (TOTP MFA)	IMPLEMENTED	LOW
Session Management	IMPLEMENTED	LOW
Role-Based Access Control	IMPLEMENTED	LOW
SQL Injection Prevention	IMPLEMENTED	LOW
XSS Prevention	IMPLEMENTED	LOW
Audit Trail with AES-256 Encryption	IMPLEMENTED	LOW
HTTPS/TLS 1.2+ Encryption	IMPLEMENTED	LOW
Firewall / WAF / DDoS Protection	IMPLEMENTED	LOW
Encrypted Backups	IMPLEMENTED	LOW
Endpoint Encryption (BitLocker)	IMPLEMENTED	LOW
Daily Backups (14-day retention)	IMPLEMENTED	LOW
Disaster Recovery (backup-based)	IMPLEMENTED	LOW
UK Data Centre Location	IMPLEMENTED	LOW
Login Rate Limiting (5 attempts / 15-min lockout)	IMPLEMENTED	LOW

2. Authentication and Access Control

2.1 Password Security

- All user passwords are hashed using bcrypt via PHP's password_hash() with PASSWORD_DEFAULT
- Legacy plaintext and MD5 passwords were bulk-migrated to bcrypt on 15 May 2026
- The legacy fallback code (MD5 and plaintext verification) has been permanently removed from the login system
- Only bcrypt verification (password_verify) is accepted for authentication
- Minimum password length of 12 characters is enforced (client-side and server-side)
- Password complexity requires uppercase, lowercase, numeric, and special characters
- All existing users were required to change their password on next login to meet the new policy
- Admin password resets via Staff Management require manager access level 9+
- Password changes are logged in the audit trail with masked values (no plaintext passwords recorded)

2.2 Multi-Factor Authentication (MFA)

- MFA is mandatory for all users and enforced at the application level
- Users who have not configured MFA are automatically redirected to the setup page
- MFA uses Time-based One-Time Passwords (TOTP) as defined in RFC 6238
- Users may choose any TOTP-compatible authenticator app (e.g. Google Authenticator, Microsoft Authenticator, Duo)
- TOTP secrets are generated using cryptographically secure random number generation
- Eight single-use recovery codes are generated during setup, hashed with bcrypt before storage
- Recovery codes are displayed once and cannot be retrieved afterwards
- MFA administration (reset capability) is restricted to senior administrators (level 9+)
- All MFA events are logged in the audit trail (setup, verification, failed attempts, recovery code usage, admin resets)

2.3 Session Management

- Sessions expire automatically after 30 minutes of inactivity
- Single-session enforcement: logging in on a new device immediately invalidates any existing session

- Session IDs are stored in the Staff_Login_Status database field for cross-session validation
- Every page request validates the session against the database record
- AJAX endpoints detect expired/invalid sessions and return JSON 401 responses (not HTML redirects)
- On logout, the session is destroyed and the database login status is cleared

2.4 Login Flow

The login process enforces the following sequence:

1. Username and password verification (bcrypt)
2. MFA verification via TOTP code or recovery code
3. Forced password change (if flagged by administrator)
4. MFA setup (if not yet configured)
5. Access to dashboard

2.5 Role-Based Access Control

The CRM implements a 10-level access control system via the Staff_Access_Level field:

Level	Role	Capabilities
1-6	Standard users / Assessors	View assigned bookings, update own records
7	Senior users	Edit bookings, view diary
8	Managers	Bulk operations, report generation
9	Senior Managers	Staff management, password resets, MFA admin, system settings, audit log
10	System Administrator	Full system access

- Access level checks are enforced on both the page level and AJAX endpoint level
- Only active staff (Staff_Current = 1) can log in; deactivated accounts are locked out

2.6 IP-Based Access Control

- File system access (job photos and documents) is restricted to connections from the Head Office public IP address
- The Head Office IP is configurable via the HO Network Settings page (level 9+ administrators)
- IP verification occurs at login and the result is stored in the session

3. Cryptography

A Cryptography Policy is in place governing the use of encryption across all systems.

3.1 Encryption in Transit

- All CRM traffic is encrypted via HTTPS with TLS 1.2+ enforced
- SSL/TLS certificates are provided via Let's Encrypt with automatic renewal
- TLS 1.0 and TLS 1.1 are disabled on the hosting server
- Head Office file sharing uses SMB 2/3 only; SMB 1 is disabled
- NTLMv2 authentication is enforced on the NAS; NTLMv1 is disabled

3.2 Encryption at Rest

- Hosted database server uses full disk encryption (FDE) at the hardware layer in ISO 27001 accredited data centres
- All hosting provider backups are encrypted
- Sensitive audit log fields are encrypted at application level using AES-256-CBC with HMAC-SHA256 integrity verification
- Endpoint devices use Windows Device Encryption / BitLocker with TPM 2.0
- The HO NAS (WD My Cloud PR4100) does not support hardware encryption; compensating controls are documented in the Cryptography Policy

3.3 Prohibited Algorithms

The following are prohibited across all systems:

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

4. Database Security

4.1 SQL Injection Prevention

- All database queries use MySQLi prepared statements with parameterised binding

- No raw user input is concatenated into SQL strings anywhere in the codebase
- Bind parameters are typed (string 's', integer 'i') for additional safety

4.2 Database Credentials

- Database connection credentials are stored in config.php on the server
- config.php is a PHP file and cannot be downloaded as plaintext by web visitors
- The database server accepts connections from localhost only (standard cPanel configuration)

4.3 Data Integrity

- Foreign key relationships link jobs, properties, clients, and status records
- Soft deletion is used for jobs (Job_Deleted flag) to preserve referential integrity
- Staff accounts are deactivated rather than deleted to preserve audit trail integrity

5. Audit Trail

The CRM maintains a comprehensive, tamper-evident audit trail via the Audit_Log_Tbl table.

Every audited action records:

Field	Description
Table_Name	Which database table was modified
Record_ID / Record_Ref	The specific record that was changed
Field_Name	Which field was modified
Old_Value / New_Value	The previous and new values (passwords are masked)
Action	Type of change (INSERT, UPDATE, DELETE, LOGIN, MFA events)
Changed_By	Staff initials of the user who made the change
Changed_Date	Timestamp of the change
IP_Address	IP address of the user at the time of change
User_Agent	Browser identification string
Change_Reason	User-supplied or system-generated reason for the change

- The audit system includes built-in error handling and a self-test function (testAuditSystem)

- Audit records are append-only; there is no facility for staff to delete or modify audit entries
- Sensitive values (passwords) are recorded as masked strings rather than actual values
- Sensitive audit fields are encrypted at rest using AES-256-CBC
- The audit log viewer requires a separate access password for an additional layer of protection
- Audit events include: INSERT, UPDATE, DELETE, LOGIN, LOGIN_FAIL, SESS_EXPIR, SESS_KICK, MFA_ENABLE, MFA_FAIL, MFA_RECOV, MFA_RESET, PW_CHANGE

6. Application Security

6.1 Cross-Site Scripting (XSS) Prevention

- All user-supplied data is escaped using htmlspecialchars() before rendering in HTML output
- This applies to all display pages, search results, form pre-fills, and modal content

6.2 Request Handling

- All form submissions use POST method for data modification
- AJAX endpoints validate session state and return appropriate JSON error responses
- Content-Type headers are set correctly on all AJAX responses (application/json)
- Session validation runs on every page load via the shared check_login.php include

6.3 Error Handling

- Database errors are caught and logged without exposing internal details to users
- AJAX error responses return generic messages, not stack traces or SQL details

7. Hosting and Infrastructure

The CRM system is hosted by Hosting Heroes on a cPanel-based shared hosting platform.

Web Hosting (Hosting Heroes):

Measure	Details	Status
Hosting Provider	Hosting Heroes	ACTIVE
Platform	cPanel, PHP 8.4, MySQL	ACTIVE

SSL/HTTPS	Let's Encrypt TLS 1.2+ enforced on all pages	**IMPLEMENTED**
Data Centre Accreditation	ISO 27001 and PCI-DSS accredited	**ACTIVE**
Full Disk Encryption	FDE at hardware layer (standard for ISO-compliant shared hosting)	**IMPLEMENTED**
Encrypted Backups	Backups encrypted and stored across geographically diverse locations	**IMPLEMENTED**
Firewall / WAF	Imunify360 and ModSecurity	**IMPLEMENTED**
DDoS Protection	Enterprise-grade DDoS protection	**IMPLEMENTED**
Backup Frequency	Daily automated backups via JetBackup	**IMPLEMENTED**
Backup Retention	14-day rolling retention; self-service restore via cPanel	**IMPLEMENTED**
Disaster Recovery	Based on robust daily backup procedures with 14-day retention	**IMPLEMENTED**
Server Location	UK data centres	**ACTIVE**
OS / Platform	CloudLinux OS with cPanel	**ACTIVE**
Patching	Critical patches applied within hours to days of alerts	**IMPLEMENTED**
Sub-processors	MailChannels (email), Acronis (backups)	**ACTIVE**

Head Office File Server (On-Premises):

Measure	Details	Status
Device	WD My Cloud PR4100 (4-bay NAS)	**ACTIVE**
Location	11 Dunkirk Business Park, Southwick, Trowbridge, BA14 9NL	**ACTIVE**
Network Access	Local LAN only; remote access disabled	**IMPLEMENTED**
Protocols	SMB 2/3 only; NTLMv2 enforced	**IMPLEMENTED**
Disabled Services	FTP, NFS, SSH, SNMP, Remote Dashboard all OFF	**IMPLEMENTED**

Web Dashboard	HTTPS redirect enabled; 10-minute access timeout	**IMPLEMENTED**
Share Access	User-level authentication enforced	**IMPLEMENTED**
Data Jurisdiction	UK (on-premises)	**ACTIVE**
Encryption at Rest	Not supported by device; compensating controls in place	**ACTIVE**

Note: Hosting Heroes confirmed that MySQL data-at-rest encryption details are not specifically confirmed at the database level. Full disk encryption at the data centre hardware layer and application-level AES-256 encryption provide the primary at-rest protection.

8. Endpoint Security

Staff access the CRM using personal devices (BYOD). The following controls are in place:

Control	Details	Status
Operating System	All endpoints run Windows 11	**IMPLEMENTED**
Disk Encryption	Device Encryption / BitLocker with TPM 2.0	**IMPLEMENTED**
Anti-Virus	Windows Security (Microsoft Defender) with real-time protection	**IMPLEMENTED**
Signature Updates	Automatic via Windows Update	**IMPLEMENTED**
OS Patching	Automatic via Windows Update	**IMPLEMENTED**
Removable Media Scanning	Automatic scan on connection via Windows Security	**IMPLEMENTED**
Local Data Storage	No CRM data stored on endpoints (web-based access only)	**IMPLEMENTED**

9. Organisational Measures

- Access to the CRM is limited to current staff only (Staff_Current flag must be set to active)
- Staff management (creating accounts, resetting passwords, deactivating users) requires manager access level 9+

- MFA administration (resetting authenticator) requires manager access level 9+
- All users must set up MFA before accessing the system; this is enforced automatically
- All users must meet the 12-character password complexity requirements
- Staff accounts are deactivated rather than deleted when individuals leave, preserving the audit trail
- Bulk data operations (e.g. bulk status updates) require manager access level 8+
- The system is accessed via a web browser; no data is stored on local devices
- Comprehensive in-application help documentation covers all security features and procedures

10. Media Disposal

- All storage media (HDD, SSD, NVMe) are securely wiped using ShredOS/nwipe prior to disposal, supporting DoD 5220.22-M standard
- Tapes are not in use
- Server-side media disposal at the hosting provider is managed under their data processing agreement

11. Supporting Policy Documents

Policy	Version	Date
Cryptography Policy	1.0	16 May 2026
Patch Management Policy	1.0	15 May 2026
GDPR Compliance Policy	1.0	15 May 2026

12. Recommendations for Further Improvement

The following enhancements are recommended to further strengthen the security posture:

Priority 1 - Application enhancements:

- Add CSRF (Cross-Site Request Forgery) tokens to form submissions

Priority 2 - Policy and process:

- Establish a formal data retention and deletion policy with scheduled reviews
- Implement a process for regular security reviews (at least annually)
- Create a staff security awareness procedure for CRM users
- Establish an incident response plan and test it periodically

13. Document History

Version	Date	Author	Changes
1.0	15 May 2026	Mark Brebner	Initial version based on full codebase audit
2.0	16 May 2026	Mark Brebner	Updated: MFA implemented, 12-char password policy, cryptography section, hosting details confirmed (backups, DR, location, firewall), NAS configuration documented, endpoint security, media disposal added

Name: Jason Lloyd Position: Director

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