

Data Security Statement

Free Clear Port Consulting LLC

Effective Date: November 20, 2025

Company Address: 30 N Gould St, Sheridan, WY 82801, United States

Website: <https://fcp-consulting.co>

Email: office@fcp-consulting.co

This Data Security Statement describes the technical and organizational measures used by Free Clear Port Consulting LLC to protect engineering files personal information project documentation and all other data entrusted to us. Our commitment is to maintain a secure environment suitable for international engineering consulting operations particularly those involving CAD files static calculations industrial designs and sensitive project materials.

1. Security Principles

Free Clear Port Consulting LLC applies industry standard best practices to ensure confidentiality integrity and availability of all data.

Our security approach is based on the following principles.

Minimum necessary access

Encrypted communication

Secure cloud infrastructure

Controlled collaboration

Regular monitoring and review

Compliance with applicable regulations in the United States and the European Union

2. Secure Cloud Infrastructure

All digital files are stored in secure cloud environments with access controls designed to prevent unauthorized access.

Storage is protected through encryption at rest and encryption during transfer.

Backups are performed regularly and stored in separate secure environments to ensure continuity in case of system failure or disaster recovery needs.

3. Access Control Procedures

Access to engineering data and personal information is granted only to team members directly involved in the project.

Access is revoked immediately when no longer required.

All systems require strong passwords and multi factor authentication.

Internal access rights are reviewed periodically to ensure compliance with security protocols.

4. Handling of Engineering Files and CAD Data

Engineering materials including CAD models drawings static calculations and technical documentation are handled with elevated protection standards.

These practices include

Encrypted transfer methods for all CAD files

Controlled download permissions

Version control systems that track edits and restore previous states

Restricted visibility so only assigned engineers can view the files

Secure archival of completed project files

We do not store engineering data on unsecured local devices.

We do not share engineering files with external parties unless required for subcontracted work under strict confidentiality controls.

5. Communication Security

All communication channels including email file sharing portals and collaboration platforms use encrypted transmission.

Sensitive data is not transmitted via unsecured channels.

Where possible data is exchanged through secure cloud links with time limited access permissions.

6. Software Security and Updates

Engineering software tools including CAD applications simulation systems and analysis tools are maintained with licensed versions and updated regularly.

Security patches are applied as soon as reasonably possible.

Third party tools used for engineering work are evaluated based on security compliance reliability and quality.

7. Monitoring and Audit

Our systems are monitored to detect unauthorized access attempts malware suspicious activity or abnormal patterns.

Internal audits are performed to verify that access rules logging procedures and storage systems comply with security standards.

8. Subcontractors and External Collaborators

If project requirements involve external specialists or engineering partners their access is governed under strict confidentiality agreements.

They may receive only the data essential for their tasks.

Before any subcontractor engagement we verify that they operate with acceptable security practices.

9. Incident Response Plan

In the event of a suspected or confirmed security breach we immediately activate our incident response procedures.

These steps include

Containment of the affected system

Identification of the cause

Protection of unaffected files

Notification of clients if required

Restoration from secure backups

Implementation of corrective measures to prevent recurrence

We take every incident seriously and prioritize client data protection at all stages.

10. Client Data Responsibilities

While Free Clear Port Consulting LLC uses strong security practices clients also play a role in maintaining data protection.

Clients must

Provide accurate information

Use secure channels for file transfer

Protect their own systems from malware

Notify us immediately of any suspected compromise on their side

Avoid sharing links files or folders with unauthorized individuals

11. Retention and Secure Deletion

Data is retained only for legitimate business reasons including project reference warranty review and compliance with legal obligations.

At the end of the retention period data is securely deleted through the following methods

Permanent removal from cloud storage

Deletion from backups during standard rotation

Elimination of temporary working files

Verification that no residual copies remain accessible

Clients may request earlier deletion of certain data when legally allowed.

12. International Data Protection Standards

Because Free Clear Port Consulting LLC serves clients worldwide we maintain security measures aligned with requirements in both the United States and the European Union.

This includes appropriate safeguards for international transfers and strong organizational controls for data originating from the European Union.

13. No Use for Unrelated Purposes

We never use project files technical documentation or personal information for unrelated activities including marketing internal product development resale or distribution.

All data is used exclusively for project execution and internal quality processes.

14. Updates to This Statement

We may update this Data Security Statement when new technologies standards or legal requirements arise.

The effective date always reflects the latest version.

Continued use of our services constitutes acceptance of updated terms.

15. Contact Information

For questions about data protection security procedures or the handling of engineering materials contact us at

Email: office@fcp-consulting.co

Address 30 N Gould St Sheridan WY 82801, United States