SECURITY

Physical Security Policy

Policy Owner: Paul Jones

Version: 2.0

Effective Date: 2021-07-06

Last Reviewed: 2026-02-24

1. Purpose

To define the physical security controls appropriate to a remote-first organization and to protect company assets and customer data from physical loss, theft, or unauthorized access.

2. Scope

This policy applies to:

- All employees and contractors
- Company-issued devices
- Work-from-home environments
- Cloud-hosted infrastructure
- Any physical equipment used to process company or customer data

Crystal Project Inc does not operate physical office locations or on-premises data centers.

3. Cloud Infrastructure Physical Security

All production systems and data are hosted in cloud environments managed by approved providers (e.g., AWS).

Physical security controls for production data centers — including facility access controls, surveillance, environmental controls, and hardware protections — are the responsibility of the cloud provider.

Cloud provider physical security assurances are reviewed as part of vendor risk management.

4. Remote Work Environment Security

Personnel are responsible for maintaining reasonable physical security of their work environment, including:

- Preventing unauthorized individuals from accessing company systems
- Securing devices when unattended
- Using screen locks and device encryption
- Avoiding exposure of sensitive information in public spaces

Work involving sensitive information should be conducted in a manner that reduces risk of shoulder surfing or unintended disclosure.

5. Device Protection

Company-issued devices must:

- Use full-disk encryption
- Require password or biometric authentication
- Be locked when unattended
- Be protected against theft or unauthorized use

Loss or theft of a device must be reported immediately in accordance with the Incident Response Policy.

6. Disposal and Reassignment of Equipment

When devices are returned to the company:

- Company data must be removed prior to reassignment or disposal.
- Devices must be securely wiped or reprovisioned before reuse.

If devices are transferred to former personnel with management approval, company access must be removed in accordance with the Access Control Policy.

7. Third-Party Physical Security

Suppliers and service providers that store or process company or customer data must maintain appropriate physical security controls.

Physical security assurances for cloud providers and critical vendors are evaluated through the Third-Party Risk Management process.

8. Exceptions

Exceptions must be documented and approved by the Policy Owner.

9. Enforcement

Violations may result in:

- Removal of system access
- Corrective action
- Disciplinary measures
- Termination of engagement where appropriate

10. Review and Revision History

Version	Date	Description	Author
1.0	2021-07-06	Initial Version	Kirsten Alexander
2.0	2026-02-24	Rewritten for remote-first, cloud-hosted model	Paul Jones