SECURITY

Access Control Policy

Policy Owner: Paul Jones

Version: 2.1

Effective Date: 2023-01-18

Last Reviewed: 2026-02-24

1. Purpose

To ensure that access to systems, infrastructure, and data is restricted to authorized individuals based on role and business need.

2. Scope

This policy applies to:

- All systems that process, store, or transmit Confidential or Customer data
- Production infrastructure
- Source code repositories
- All employees and authorized contractors

3. Access Control Principles

Crystal Project applies the following principles:

- Least privilege
- Role-based access control (RBAC)
- Unique user identities
- Multi-factor authentication (MFA) required for all workforce identities
- Prompt removal of access upon termination or role change

Access not explicitly granted is denied by default.

4. Identity and Authentication

- All personnel must use unique user accounts.
- Shared user accounts are prohibited except for technical service accounts.
- Google Workspace is used as the primary identity provider where applicable.
- MFA is required for all workforce identities and for all privileged access. Exceptions require documented approval from the Policy Owner.
- Passwords must comply with organizational standards and be protected using appropriate cryptographic controls.

5. Provisioning of Access

Access is granted based on role and business need.

Provisioning is performed by authorized administrators using role-based groups where possible.

Access requests may be communicated through internal communication channels (e.g., Slack, email) and must be approved by management or the Policy Owner prior to granting privileged or production-level access.

System audit logs and platform-level access records provide evidence of access grants and modifications.

6. Modification of Access

When an employee changes roles:

- Access rights must be reviewed.
- Access not required for the new role must be removed.

Management is responsible for initiating access adjustments when role changes occur.

7. Deprovisioning of Access

Access must be removed promptly upon:

- Termination of employment

- End of contract
- Role change where access is no longer required

Maximum time for production access removal is 24 business hours.

Deprovisioning may occur immediately for high-risk or privileged roles.

User IDs must not be re-used.

8. Privileged Access Management

Administrative or privileged access:

- Is restricted to personnel with defined operational need
- Requires MFA
- Is limited in scope
- Is subject to logging and monitoring through system-level audit capabilities

9. Access Reviews

Access rights are reviewed periodically to ensure they remain appropriate based on role and business need.

Access reviews are conducted by management and include:

- User accounts
- Administrative accounts
- Service accounts where applicable

Review results are documented and retained.

10. Source Code Access

Access to source code repositories:

- Is restricted based on role

- Is controlled through centralized version control systems
- Does not allow anonymous or public modification of private repositories

Protected production branches restrict direct modification.

11. Network and Remote Access

Remote access to production systems must:

- Be encrypted
- Require authentication
- Be restricted to authorized users

Guest or public network access must be logically separated from production systems.

12. Exceptions

Exceptions must:

- Be documented
- Include justification
- Be approved by the Policy Owner

13. Violations and Enforcement

Violations may result in:

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

14. Review and Revision History

Version	Date	Description	Author
1.1	2023-01-18	Prior revision	Paul Jones
2.1	2026-02-24	Aligned to operational practice	Paul Jones