

Security Program & Operations

How Cyber Crucible operates its security program — change management, patch and vulnerability management, disaster recovery and business continuity, incident and breach response, and endpoint control — described for vendor-risk reviewers. States plainly what is documented and what is provided under NDA, and claims no certifications.

- [Does Cyber Crucible have a change management process?](#)
- [Does Cyber Crucible have a patch management program?](#)
- [Does Cyber Crucible have a disaster recovery and business continuity plan?](#)
- [Does Cyber Crucible have an incident response and breach-notification process?](#)
- [How does Cyber Crucible secure and control endpoints?](#)
- [Which security policies does Cyber Crucible maintain, and how do I request them?](#)

Does Cyber Crucible have a change management process?

Short answer: Yes. Production changes follow a documented change-management process with review, testing, and approval. Because the product operates at the kernel level, change discipline is treated as a security control rather than merely an engineering practice.

What the process covers

Changes to application code, kernel drivers, server configurations, and supporting infrastructure move through defined lifecycle stages: security requirements are set at design; source is version-controlled and secrets are never embedded in cleartext; automated testing validates changes before promotion; and production changes receive formal review and approval. Segregation of duties is maintained, so the author of a change is not its sole approver. Server baselines follow approved configuration guides, and unused services are disabled where practical.

Emergency and driver changes

Emergency changes use an expedited path that still requires authorization, targeted testing, and a post-implementation review. Windows kernel drivers undergo internal quality assurance and are submitted for Microsoft's Windows Hardware Compatibility Program (WHCP) certification before release — an independent, external check of the most privileged component.

Framework alignment and the honest boundary

The process aligns to NIST SP 800-53 (CM family) and ISO/IEC 27001:2022 A.8.32. Cyber Crucible does not claim any certification. The detailed change-management procedure and supporting evidence are provided to reviewers under NDA.

Does Cyber Crucible have a patch management program?

Short answer: Yes. A risk-based patch and vulnerability-management program keeps software, kernel drivers, servers, and endpoints current, and findings are tracked to resolution.

How it works

Continuous automated security testing runs within the development pipeline, risk-based manual penetration testing is performed with an annual floor, and event-triggered testing runs on every significant change, covering both internal and external networks. Security patches and hot-fixes are applied per vendor recommendation, and owner groups are responsible for staying current on applicable patches. Removable and portable media are held to the same protection and scanning as fixed media.

Prioritization and deployment

Findings are prioritized by severity and exploitability, with actively exploited vulnerabilities handled through an expedited, out-of-band path. Patches follow the change-management process — validated before promotion to production — and kernel-driver updates are re-validated through Microsoft WHCP before release.

Framework alignment and the honest boundary

The program aligns to NIST SP 800-40, NIST SP 800-53 (SI-2, RA-5), CIS Control 7, and ISO/IEC 27001:2022 A.8.8. No certification is claimed. Specific target remediation windows and remediation evidence are provided to reviewers under NDA.

Does Cyber Crucible have a disaster recovery and business continuity plan?

Short answer: Yes. Cyber Crucible maintains a tested disaster-recovery plan owned by IT management and an architecture built for high availability. Because threat prevention runs locally on the endpoint, endpoint protection continues even during a management-backend outage.

Resilience by architecture

The management backend is built with redundant, replicated storage so that the loss of an individual node does not cause data loss or downtime. The published Service Level Agreement commits to 99.9% monthly availability for the management and reporting backend, exclusive of scheduled maintenance and causes beyond reasonable control. Endpoint protection itself is unaffected by a backend outage.

Backups and contingency planning

Data is continuously replicated and backed up to secure offsite storage using distinct privileged credentials, with backups protected against ransomware through offline or immutable handling and tested on a regular basis. The plan maintains a computer emergency response plan, a succession plan, a data-criticality study, and a criticality-of-service list, and incorporates business-impact analysis, recovery strategies, a communication plan including customer notification, and defined recovery objectives. Testing includes table-top exercises and recovery drills.

Framework alignment and the honest boundary

The plan aligns to NIST SP 800-34 and ISO/IEC 27001:2022 A.5.29-A.5.30. Cyber Crucible defines recovery-point and recovery-time objectives for the backend; the specific target values, and the plan itself, are provided to reviewers under NDA. Because protection executes locally, endpoint defense continues with effectively no recovery-time gap during a backend outage or in an air-gapped deployment.

Does Cyber Crucible have an incident response and breach-notification process?

Short answer: Yes. A documented data-breach response process defines the roles and steps for responding to a suspected theft, breach, or exposure of protected data, including customer notification. A committed notification timeframe can be set by contract for regulated customers.

The response process

A suspected incident is reported immediately through internal channels monitored by the Information Security function. On identification, access to the affected resource is removed and an incident response team chaired by executive management is convened. Forensic investigators and experts, provided through Cyber Crucible's cyber and technology insurance, determine how the incident occurred, the data involved, the parties affected, and the root cause. A communication plan is developed with Legal, Communications, and Human Resources to notify staff, the public, and affected parties as appropriate — including customer notification through a mutually agreed channel — followed by a post-incident review.

Support response and notification

Customer-facing incidents are tracked against the published SLA severity tiers (SEV1 through SEV4), and a breach or incident notification timeframe can be committed contractually for regulated customers.

Framework alignment and the honest boundary

The process aligns to NIST SP 800-61 and ISO/IEC 27001:2022 A.5.24–A.5.26. No certification is claimed. The full incident-response and breach-notification procedure is provided to reviewers under NDA.

How does Cyber Crucible secure and control endpoints?

Short answer: In two ways. The product itself is autonomous endpoint prevention operating at the kernel layer, and Cyber Crucible controls its own corporate and engineering endpoints under a formal program. Both rest on building the most privileged code in-house.

Product endpoint protection

The product provides autonomous prevention against ransomware, in-memory (fileless) attacks, and process injection, enforced at the kernel layer. It is deliberately decoupled from operating-system libraries, so when attackers compromise or hijack those libraries in memory the product continues to run, enforce, and report. Because detection and response execute locally, protection continues during a management-backend outage or in a deliberately air-gapped deployment.

Supply-chain integrity and independent validation

The discovery algorithms, kernel heuristics, sensors, and drivers are engineered and maintained in-house; no unverified third-party libraries or hidden telemetry hooks are embedded in the software. Because the highest-privilege component is proprietary, an entire class of third-party supply-chain exposure is removed rather than merely managed. All Windows kernel drivers are validated and signed under Microsoft's Windows Hardware Compatibility Program (WHCP).

Corporate endpoint controls

Managed endpoints follow approved secure configuration baselines, run endpoint protection and scanning, and apply the same controls to removable and portable media as to fixed media, with unauthorized media use restricted. Software installation is governed by policy, data at rest on endpoints is encrypted, and endpoints are kept current under the patch-management program.

Framework alignment and the honest boundary

Endpoint controls align to the CIS Critical Security Controls (v8) and NIST SP 800-53 (SI-3, CM-2, MP-7). No certification is claimed. Detailed configuration standards and evidence are provided to reviewers under NDA.

Which security policies does Cyber Crucible maintain, and how do I request them?

Short answer: Cyber Crucible maintains a full information-security policy set — covering acceptable use, access and authentication, encryption, change management, disaster recovery, incident and breach response, data retention and destruction, and more. Policies and supporting evidence are available to reviewers under NDA.

Representative policy areas

The policy set spans acceptable use and ethics; access, authentication, and remote access; encryption and key protection; secure development and change management; server and endpoint security; disaster recovery and business continuity; incident and breach response; and data retention, destruction, and email retention. Program summaries for compliance, audit, and AI/SDLC governance are maintained alongside the policies.

What is public and what is under NDA

Public knowledge base pages describe the existence, principles, and framework alignment of each program so that a reviewer can understand the posture at a high level. The specific policy documents, configuration standards, exact figures (such as retention schedules and recovery objectives), and audit evidence are confidential and provided under a mutual NDA, alongside the prepared vendor due-diligence package.

How to request them

Reviewers can request the security policy set, the prepared vendor package, and supporting evidence from **dpo@cybercrucible.com**. Cyber Crucible's standard mutual NDA is available if one is not already in place. No certification is claimed for any framework; the documentation explains how the architecture and controls support each obligation.