

RECOVER WITH CONFIDENCE

Implement a plan that leaves zero doubt about recovery.


Avoid the damage that downtime and data theft can cause. Prepare today for resilience tomorrow with our Cyber Recovery Checklist.





PHASE 1

Phase 1 | 30 Days


Establish the Foundation.
What you can do NOW to protect your business.

-  Create protection and retention policies for all workloads.


-  Use immutable storage.

-  Implement 3-2-1 backup strategy — three copies in two formats; one offsite including a virtual and/or physical air gap; SaaS isolation vital.

-  Apply security controls (e.g. MFA, MPA, network segmentation, RBAC, encryption).

-  Consider purpose-built hardened appliances.

-  Enable AI-powered anomaly detection.


-  Turn on malware detection and retention rules.


-  Update software and security patches (ongoing).


PHASE 2


Phase 2 | 60 Days


Proactively Manage Risk.
Focus on people, processes, and technology.


-  Identify “missing” critical assets.

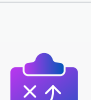
-  Conduct dark data assessment.

-  Discover and classify sensitive data.

-  Identify and monitor high-risk end-user behavior.

-  Create an isolated recovery environment (IRE or clean room).


-  Develop recovery runbooks, prioritizing order of operations.


-  Integrate with SecOps and establish incident response playbooks (e.g. SIEM / SOAR / XDR integration).


PHASE 3


Phase 3 | 90 Days

Refine. Rehearse. Adapt.

-  Adjust data protection policies to drive to 100% backup success, in accordance with SLAs.

-  Fine tune AI-powered anomaly detection (eliminate false positives/negatives).

-  Run tabletop exercises, including non-disruptive recovery rehearsals.

-  Rehearse recovery and validate results.

[See the Complete Cyber Recovery Checklist >](#)