Microsoft 365 Cyber Resilience Checklist

Action Item	Assigned to	Due Date	Notes	✔
ANTICIPATE (PREPARE FOR THREATS)				
Regularly review emerging threats and adjust standards.				
Partner with vendors that support rapid threat response.				
Use extensible platforms to respond quickly to new risks.				
Establish internal processes for threat intelligence updates.				
WITHSTAND (PREVENT AND MINIMIZE DAMAGE)				
Least privilege access				
Create custom admin roles with “just enough” access.				
Monitor and manage Entra Apps and their permissions.				
Remove unused or over-privileged accounts.				
Secure configuration				
Configure tenant and policies to align with best practices.				
Monitor for configuration drift and enforce baselines.				
Implement change management (test before deploying).				
Detect and test Microsoft 365 updates for security impacts.				
Monitor sharing and collaboration				
Monitor and remediate risky external and guest users.				
Limit and review high-risk sharing (e.g., anonymous links).				
Audit Exchange for suspicious mailboxes (auto-forwarding, disabled audit logging).				

Action Item	Assigned to	Due Date	Notes	✔
RECOVER (BOUNCE BACK QUICKLY)				
Backup all Microsoft 365 configurations (Entra, Intune, Defender, Teams, etc.).				
Test and maintain rollback capabilities for configurations.				
Delegate recovery roles with least privilege access.				
Use enhanced management tools for faster recovery execution.				
ADAPT (IMPROVE CONTINUOUSLY)				
Enable custom reporting for evolving security needs.				
Automate security tasks and remediations.				
Invest in extensible platforms for rapid threat response.				
Review access regularly and deprovision unused accounts.				
Track and test updates in a controlled test environment.				