INCIDENT RESPONSE PLAN

IRP Testing Checklist

CYBER READINESS INSTITUTE

Write in the date you tested each step.

Testing Step	Action / Scenario To Test	Success Criteria	Testing Frequency	Date Tested
1. Verify Reporting Speed	Simulate an employee reporting an unexpected MFA prompt or suspicious invoice email.	Employee alerts Cyber Leader within 10 minutes using approved channel.	Every 6 months	
2. Test Emergency Communications	Test out-of-band communication (phone or messaging) assuming primary email is offline.	All people listed on the IRP acknowledge emergency test message within 15 minutes.	Every 6 months	
3. Test Network Containment	Walk through immediate containment steps for an infected workstation or smart device.	Non-technical staff correctly state how to disconnect device without shutting down.	Every 6 months	
4. Practice AI Scenarios	Conduct a tabletop drill simulating an AI voice-clone or realistic phishing email from a colleague	Team uses trusted voice verification channel before moving funds or changing vendor information.	Every 12 months	
5. Annual Plan Audit	Review contact details, roles, escalation procedures, alternative communication methods, and supporting tools following personnel or technology changes.	Updated IRP approved by leadership and distributed to key team leads.	Every 12 months	

© 2026 Center for Global Enterprise (CGE). Cyber Readiness Institute is an institute of CGE. Free to use and share with attribution.

INCIDENT RESPONSE PLAN

IRP Testing Checklist

CYBER READINESS INSTITUTE

If you want to list more tests, add them here.

Testing Step	Action / Scenario To Test	Success Criteria	Testing Frequency	Date Tested

© 2026 Center for Global Enterprise (CGE). Cyber Readiness Institute is an institute of CGE. Free to use and share with attribution.