BITS CYBER

Secure Business Innovation

BITS Cybersecurity Insurance Checklist

Aligned with the BITS Cybersecurity Control Framework & Business Change Tolerance (BCT)

To qualify for cyber insurance and protect your business from disruption carriers expect proof that you've addressed core areas of cybersecurity. This checklist translates those expectations into business-friendly actions.

✅ We verify identity in multiple ways.

Only authorized people can log into our systems thanks to multi-factor authentication (MFA). This applies to remote access, admin tools, and email. → IDA.3

✅ We protect all devices that access our systems.

Laptops, servers, and cloud environments are covered by next-generation antivirus (NGAV) with Endpoint Detection & Response (EDR). We get alerts when something suspicious happens. → TAC.1, TAC.3

✅ We define roles and assign access accordingly.

We understand everyone's role in the business and ensure access to data and systems matches responsibilities. Admin rights are limited, and role-based access is reviewed regularly. → RDF.1–RDF.3

✅ We remove access when people leave or change roles.

Employee and contractor offboarding is structured, fast, and secure. We remove access, collect equipment, and update permissions. → CHG.2

✅ We log and monitor system activity.

If something goes wrong, we can trace what happened and who was involved. Logs are centralized, monitored, and stored securely. → TAC.3, TDL.3, EBM.3

✅ We secure remote and cloud access.

Remote employees connect using trusted, encrypted channels (VPN or SASE). Admin access to cloud platforms is restricted and monitored. → TAC.1, TAC.4

✅ We back up our data regularly.

Critical data is backed up to secure, off-site or cloud locations. We track recovery time and validate backups regularly. → BDR.1–BDR.2

✅ We test our ability to recover from disruption.

We simulate outages and validate that we can recover quickly with minimal impact. → BDR.3, SI.1

✅ We know where our critical data lives.

We maintain a current inventory of all the places our business data is stored—cloud, servers, and physical media—so we can protect it appropriately. → TDL.1–TDL.2

✅ We know which vendors have access to our data.

We track every vendor or platform that handles our data. We assess their risk and monitor their compliance. → TDP.1–TDP.2

✅ We train our team to spot risk.

Employees are trained on phishing, data protection, and how to report suspicious activity. Security awareness is part of onboarding and culture. → SBA.2–SBA.3

✅ We have a documented incident response plan.

We know what to do if there's a breach. Roles are assigned, steps are defined, and we've rehearsed how to respond. → BDR.2, SI.4