Everyday Identity

Trust Nothing. Verify Everything.
Protect Everyone.

10 Essential ‘Be Safe’ Zero Trust Checklist

1 Enable Multi-Factor Authentication (MFA) Everywhere

□ Protect all accounts—especially privileged ones—with MFA.

2 Centralize Identity Management

□ Use a single IAM platform (Okta, Microsoft Entra ID, Ping) to unify access control.

3 Adopt Least Privilege Access

□ Give users the minimum access they need—nothing more, nothing longer than necessary.

4 Implement Just-in-Time (JIT) Access for Admins

□ Eliminate standing admin privileges; grant elevated access only when required.

5 Verify Device Health Before Access

□ Require encryption, EDR, and compliance checks on laptops, mobiles, and endpoints.

6 Microsegment Networks & Applications

□ Divide environments into zones to contain lateral movement and limit attack blast radius.

7 Continuously Monitor & Log Activity

□ Track logins, file access, and privilege escalations for anomalies and suspicious behavior.

8 Protect Against Insider Threats

□ Use adaptive authentication, session monitoring, and access certifications.

9 Encrypt Data Everywhere

□ Apply strong encryption for data in transit and at rest to assume breach resilience.

10 Review & Evolve Policies Regularly

□ Zero Trust isn’t “set it and forget it”—continuously adapt controls to emerging threats.

💡 **Quick Tip: Zero Trust works best when everyone understands it. Train your team regularly—awareness and culture are just as critical as technology.**