ENVORN DIGITAL · FREE CHECKLIST

Cloud Security Checklist

30 essential controls for small and mid-sized teams · 30 items

Identity & access

- ☐ MFA enforced for every user, especially admins
- ☐ No daily work done with root/owner accounts
- ☐ Least-privilege roles; no wildcard admin permissions
- ☐ Access reviewed quarterly; leavers removed same day
- ☐ Single sign-on for cloud consoles and SaaS where possible

Data protection

- ☐ Encryption at rest enabled for storage and databases
- ☐ TLS for all data in transit
- ☐ Keys managed in a KMS; rotation scheduled
- ☐ No public storage buckets unless intended and reviewed
- ☐ Sensitive data classified and its location known

Network

- ☐ Default-deny security groups / firewalls
- ☐ Databases in private subnets only
- ☐ Admin access via VPN, bastion or zero-trust access, never open SSH/RDP
- ☐ WAF in front of public web apps
- ☐ DDoS protection / CDN enabled for public sites

Secrets & code

- ☐ No secrets in source code or repos
- ☐ Secrets stored in a secrets manager
- ☐ Dependency and container image scanning in CI
- ☐ Infrastructure defined as code and peer reviewed
- ☐ Production changes go through approval

Monitoring & response

- ☐ Audit logs enabled and retained 1 year+

- ☐ Alerts for root login, policy changes and unusual spend
- ☐ Centralized logging / SIEM
- ☐ Incident response plan with named contacts
- ☐ Tabletop exercise run in the last 12 months

Resilience & governance

- ☐ Backups automated, encrypted, stored in another region/account
- ☐ At least one immutable backup copy
- ☐ Restore tested in the last quarter
- ☐ RTO/RPO defined for critical systems
- ☐ Compliance requirements (PCI, HIPAA, GDPR) mapped to controls

Free resource from Envorn Digital · envorndigital.com · Share freely with attribution. General information only, not professional advice.