FREE RESOURCE · GCC SME EDITION

The GCC SME Cybersecurity Checklist

40 practical checks across five security domains, written specifically for businesses operating in Saudi Arabia, the UAE, Bahrain, and the wider GCC. Work through each section honestly — the value of this checklist comes from an accurate picture, not a flattering one.

01 Security Governance and Strategy

Policies, ownership, and the decision-making structure everything else depends on.

- A documented security policy exists and is communicated to all staff
- A specific person or role is accountable for security decisions
- Security risks are reviewed by leadership at least quarterly
- An annual security budget and roadmap exists
- New employees receive a security briefing during onboarding
- A risk register is maintained and reviewed on a regular cycle
- Security responsibilities are written into relevant job descriptions
- Leadership has visibility into the organisation's current security posture

02 Access Control and Identity

Who can access what, and how tightly that is controlled.

- Multi-factor authentication (MFA) is enabled for all business email and cloud accounts
- A formal offboarding process removes access on the day of departure
- Access follows least-privilege principles for sensitive systems and data
- Passwords are managed through a company-standard password manager
- Privileged/admin accounts are limited to those who genuinely need them
- Shared logins are avoided in favour of individual, attributable accounts
- Remote access to company systems requires a secure connection (VPN or equivalent)
- Access permissions are reviewed periodically, not just granted and forgotten

03 Data Protection and Privacy

Covers the core requirements of Saudi PDPL, UAE FDPL, SAMA, and NCA.

- Personal data collected and stored by the business has been mapped
- A privacy notice accurately describes what data is collected and why
- A lawful basis exists for each significant category of data processing
- Data subject rights requests (access, deletion, correction) have a defined process
- Vendor and processor contracts include data protection clauses
- A data retention schedule exists and is enforced
- Cross-border data transfers are assessed against applicable restrictions
- A breach notification procedure is ready to act on within 72 hours

04 Incident Response and Recovery

How quickly and effectively the business recovers when something goes wrong.

- Backups follow the 3-2-1 rule (3 copies, 2 media types, 1 offsite) and are tested
- A documented incident response plan exists and has been exercised
- Staff receive regular security awareness training, not a one-off session
- Critical systems are patched within a defined SLA
- A clear escalation path exists for suspected security incidents
- Business continuity plans cover realistic disruption scenarios
- Phishing simulations or equivalent awareness testing are run periodically
- Post-incident reviews are conducted to capture lessons learned

05 Regulatory Compliance

The documentation and evidence that protect you under scrutiny.

- Applicable regulatory frameworks (PDPL, UAE FDPL, SAMA, NCA, etc.) have been identified
- A compliance gap assessment has been conducted in the last 12 months
- Audit-ready documentation and evidence of controls is maintained
- A named person is accountable for regulatory compliance
- Third-party/vendor risk is assessed against relevant compliance requirements
- Employee training records for compliance-relevant topics are maintained
- Regulatory changes are actively monitored, not discovered after the fact
- Prior audit or assessment findings have been tracked through to closure

Found more gaps than you expected? That is normal, and it is exactly what a free, no-obligation consultation with Code Defence is for. We will help you turn this checklist into a prioritised plan. **codedefence.in/contact**