Multi-Factor Authentication Policy — Remote Access

MFA Policy for Remote Server Access Purpose: This policy mandates the use of multi-factor authentication (MFA) for all remote access to servers, including SSH, RDP, VPN, bastion/jump hosts, and any administrative consoles that provide access to production or sensitive environments. Policy Statement: All users, contractors, and service accounts that have remote access to infrastructure managed by the organization must authenticate using at least two distinct factors: something they know (password) and something they have (authenticator app, hardware token, or SMS where applicable) Where possible, hardware security keys or authenticator apps (TOTP) are preferred over SMS. Enforcement and Eviden The organization enforces this policy through Identity Provider (IdP) configuration, workspace/team settings, VPN/bastion settings, and cloud IAM controls. Evidence of enforcement includes: (1) workspace/team setting showing MF enforced, (2) audit logs demonstrating MFA-protected sign-ins or sessions, and (3) a list of users and their 2FA enrollment status. Exceptions: Any exceptions must be documented and approved by security leadership with compensat controls in place. Contact: Security Team — security@example.com