**Certificate Revoke Request Guidelines**

**1. Understanding the Request**

Each revoke request must begin with a clear understanding of the intent and scope of the action. Certificate revocation can impact production services, integrations, and application uptime — therefore, every request must be validated for completeness and accuracy before proceeding.

**Checklist:**

* **Type of Revocation:**
  + ☐ Historical certificate revocation
  + ☐ Current active certificate revocation
* **Request Completeness:**
  + ☐ Certificate details provided (CN, SANs, expiry date, environment)
  + ☐ Environment specified — *SIT / DEV / PAT / PROD*
  + ☐ Reason for revocation clearly documented (e.g., decommission, replacement, compromise)
  + ☐ TAO (Technical Approval Officer) approval completed and attached
* **Verification:**
  + ☐ Confirm requester identity and authorization
  + ☐ Ensure no dependencies are missed (e.g., F5, load balancer, linked certificates)

**2. Effective Due Diligence**

Before processing the revocation, due diligence must be performed to prevent unexpected outages or service disruptions.

**Validation Steps:**

* **DNS & Environment Check:**
  + ☐ Verify that the DNS entry linked to the certificate is currently active.
  + ☐ Check whether the domain or application is still in use.
* **Application Impact Assessment:**
  + ☐ Confirm whether the application using the certificate is being decommissioned.
  + ☐ If yes, ensure a formal **Decommission (Decom) Request** is raised and approved.
* **F5 and Server Status:**
  + ☐ Check the F5 VIP or pool status for dependencies.
  + ☐ Confirm if the certificate is still deployed on any server or F5 device.
* **Replacement Validation:**
  + ☐ Determine if a new or modified version of the certificate has been deployed.
  + ☐ If yes, confirm deployment success before revocation of the old version.
* **Change Management:**
  + ☐ For PAT and PROD certificates, validate if a **Change Record (CR)** is required.
  + ☐ Ensure CR is approved prior to certificate revocation.

**3. Delivery and Communication Commitments**

Timely and transparent communication ensures accountability and SLA compliance throughout the certificate lifecycle.

**Process Commitments:**

* ☐ Follow SLA timelines for revoke requests based on environment priority.
* ☐ Maintain clear communication if clarifications or additional information are required.
* ☐ Document all validation steps and attach logs/screenshots where applicable.
* ☐ After revocation, confirm completion to the requester and relevant stakeholders via email.
* ☐ Archive request details and communication trail for audit reference.