**ServiceNow Pre-Clone Checklist (Granular)**

**1. Confirm Clone Scope and Timing**

* Identify source instance (e.g., **prod12345**).
* Identify target instance (e.g., **dev12345** or **test56789**).
* Choose **clone date/time** that minimizes disruption (usually off-hours).
* Communicate timing to stakeholders and developers.
* Block off time on project timelines for post-clone validation and remediation.

**2. Backup Important Data on Target**

* Export any **in-progress work** (update sets, custom tables, test data).
* Export any custom scripts, integrations, or configurations not yet committed to source control or update sets.
* Capture snapshots of **update sets**, **scripted components**, and **form changes**.
* Export records from tables like:
  + sys\_email (emails)
  + sys\_journal\_field (comments/notes)
  + task or incident (demo or test tickets)
* Export records from any **custom tables** or **non-clone-preserved** data sets.

**3. Disable Sensitive or Time-based Automations**

* Disable **Email Sending**:
  + Uncheck **Email sending enabled** in **System Mail > Email Properties**.
  + Optionally, use an **email filter script** to block outbound emails.
* Disable **Scheduled Jobs**, including:
  + Scheduled script executions
  + Inbound email actions
  + Scheduled reports
* Disable **MID Servers** or integrations in target (to prevent unintended traffic or updates).
* Disable **Notification Rules** for clone period (if not already covered by email property).

**4. Prepare Clone Exclusion Rules**

* Review and update **clone exclusion rules**:
  + sys\_clone\_exclude table
  + Common exclusions:
    - sys\_user (users)
    - sys\_user\_role (roles)
    - sys\_attachment
    - sys\_email
    - audit, syslog, and sys\_journal\_field
    - Custom tables (e.g., for test data)
* Verify **exclusion list aligns** with compliance and internal policies (e.g., removing sensitive data like PII or PHI).
* Add exclusions for **large or unnecessary tables** that may slow down the clone.

**5. Validate Target Instance Readiness**

* Ensure the target instance is **idle and not actively used**.
* Notify users the instance will be **overwritten and inaccessible** during the clone.
* Pause any **external system integrations** with the target.
* Confirm **sufficient disk space** and system health via HI > Instance Health Dashboard.

**6. Communicate & Confirm Approvals**

* Get **managerial or change advisory board approval**, especially if cloning from prod.
* Log a **change request or service request** internally, if applicable.
* Notify users, developers, and QA teams about:
  + What will be overwritten
  + What will be preserved
  + Downtime expectations
* Schedule a follow-up **post-clone validation** session.

**7. Submit Clone Request via HI**

* Navigate to **HI Service Portal > Manage Instances > Clone Instance**.
* Select source and target instances.
* Choose backup (most recent or select older).
* Configure:
  + Clone exclusions
  + Email settings
  + Optional post-clone scripts
* Confirm and submit the request.

**8. Optional – Run a Pre-Clone Script (if applicable)**

* If you have logic to clean up or tag records pre-clone, run your **custom pre-clone script**.
  + Example: Flagging test records
  + Obfuscating emails
  + Backing up config in a separate table