PCA 2011 Revocation Readiness Worksheet

ONE DEVICE CLASS · BEFORE AUTHORIZATION · GATES 1 TO 4

Device class: _____ Device count: _____ Date: _____ Completed by: _____

GATE 1 — PREREQUISITE STATE

2023 certificate in DB and PCA2023-signed boot manager? Firmware can apply DB and DBX updates?
Events 1036 and 1799 seen: [ ] yes [ ] no UEFICA2023Status = Updated: [ ] yes [ ] no
Controlled reboot test passed: [ ] yes [ ] no Firmware vendor confirmation (devices that failed): _____

GATE 2 — COMPATIBILITY INVENTORY

Boot-test result per dependency (PASS / FAIL / NOT TESTED):
Recovery USB: _____ CD/DVD: _____ PXE / network boot servers: _____
Secure Boot VM templates: _____ Disk-encryption products: _____
KB5025885 known-issues checked: [ ] yes [ ] no Date: _____

GATE 3 — ENCRYPTION READINESS

BitLocker recovery keys escrowed before the change: [ ] yes [ ] no
Third-party encryption vendor statement (product, version, reference): _____

GATE 4 — PRE-ENFORCEMENT RECOVERY PROOF

Failed-boot device recovered on one device of each type: [ ] yes [ ] no
Device model(s) tested: _____ Test date: _____
Recovery flash drive created before DBX step: [ ] yes [ ] no
Evidence reference: _____

Microsoft has not announced an enforcement date. This worksheet does not assume one.

Authorize, Pilot, Verify

ONE DEVICE CLASS · GATES 5 TO 8 · AUTHORIZATION AND CLOSURE

GATE 5 — AUTHORIZATION (BEFORE)

Named approver: _____ Role: _____
Criteria applied and date of recorded decision: _____

GATE 6 — ENFORCEMENT DECISION (BEFORE)

[ ] ENFORCE on a pilot by device class: _____
[ ] DEFER with documented exposure. Accountable owner: _____
[ ] BLOCK until recovery dependencies are remediated: _____
Open exposure stated: _____

GATE 7 — ENFORCEMENT EVIDENCE (AFTER, PILOT)

Revocation took effect on each pilot device?
Event 1037 seen: [ ] yes [ ] no DBX read-back returns True: [ ] yes [ ] no
Run by: _____ Date: _____

GATE 8 — POST-REVOCATION RECOVERY PROOF (AFTER, PILOT)

Recovery works on the pilot with no boot manager signed under PCA 2011 in the path?
Rebuilt media boot-tested after revocation: [ ] yes [ ] no
PXE servers updated and tested: [ ] yes [ ] no Evidence reference: _____
Condition for widening: [ ] PASSED, widen to the rest of the class [ ] NOT PASSED, do not widen

A completed worksheet is a record for one device class at one point in time. Reassess after material change to media, firmware or boot servers. or boot servers.