VENTEX CONNECT

PILOT LAUNCH KIT / PUBLIC METHOD / 2026

PILOT LAUNCH KIT

Templates and evidence for a controlled 30-day pilot

STATUS / PUBLIC WORKING DOCUMENT

Working method, not an audit, certification or legal advice.

VERSION 1.0 / 13 AUGUST 2026 / ventex-connect.com

01

How to use this kit

The kit runs from initial qualification to a defensible go, iterate or stop decision. Every template creates a named evidence item.

WORKING PRINCIPLE

Set the objective and protection boundary first, configure technology second, then observe real workflows. A checklist never creates a security claim.

OUTCOME

The output is a pilot record, Evidence Matrix, final report and optional anonymised case study.

- Every decision has a Pilot Owner.
- Participants accept boundaries before launch.
- Only observed outcomes are published.

RULE / CLAIM = OBSERVATION + DATE + OWNER + ARTEFACT

02

Pilot fit in 20 minutes

The first call is a qualification exercise, not a sales performance.

REQUIRED

- Named sponsor and operational Pilot Owner
- 5 to 20 participants using approved or synthetic data for 30 days
- One real workflow and a reachable fallback channel
- No expectation that the pilot replaces legal or internal approval

STOP BEFORE LAUNCH

- Production secrets without an approved protection model
- Unclear responsibility for users, devices or incidents
- Expectation of certification or transferred liability
- No reachable fallback channel

03

Participant and use-case matrix

A useful cohort is representative enough to reveal friction and small enough for controlled support.

COHORT

- Sponsor - owns the continuation decision
- Pilot Owner - daily contact and approvals
- Operators - 3 to 12 users of the actual workflow
- IT/Security - devices, identities and incidents
- Observer - compliance or workers council when required

USE-CASE SCORE

- Criticality 1-5
- Frequency 1-5
- Coordination need 1-5
- Data sensitivity 1-5
- Adoption risk 1-5; high scores constrain the scope

04

Pilot charter

The charter is the common sign-off record. It prevents silent expansion of scope.

REQUIRED FIELDS

- Organisation, pilot name and dates
- Sponsor, Pilot Owner and technical contact
- Target workflow and explicitly excluded workflows
- Participants, device classes and permitted data
- Success criteria, stop criteria and fallback channel

APPROVAL

Signed or traceable digital acceptance by sponsor, Pilot Owner and VENTEX Pilot Lead. Every change records date, reason and approver.

DO NOT START WHILE THE PROTECTION BOUNDARY OR STOP CRITERIA ARE OPEN

05

Data and confidentiality boundary

This is an operational drafting aid. Legal review and any data protection impact assessment remain the organisation's responsibility.

PERMITTED

- Synthetic or explicitly approved sample data
- Named file types and size limits
- Personal data only with documented basis and approval
- Screenshots only with consent and redaction review

NOT PERMITTED

- Classifications outside pilot approval
- Credentials, private keys or production tokens
- Hidden performance or employee monitoring
- Third-party data without a lawful basis

06

Kick-off agenda - 60 minutes

A disciplined launch establishes a shared model and immediately tests the fallback route.

00–20

- 00-05 objective, boundary and owners
- 05-12 device and identity check
- 12-20 data classes and prohibited content

20–60

- 20-35 perform the core workflow
- 35-45 exercise fallback and device revocation
- 45-52 feedback and incident channel
- 52-60 confirm success criteria

07

Roles and escalation

Every security or operational decision has exactly one decision owner and a reachable deputy.

COMPACT RACI

- Sponsor - accountable for continuation
- Pilot Owner - responsible for daily operation
- VENTEX Pilot Lead - responsible for product support
- Security Contact - consulted on security events
- Participants - informed and responsible for feedback

SEVERITY

- SEV-1 possible disclosure or identity misuse - stop immediately
- SEV-2 core workflow blocked - assess within 60 minutes
- SEV-3 limited defect with workaround - next business day
- SEV-4 improvement - backlog

08

Outreach email – first contact

Subject: Controlled 30-day pilot for secure operational communication

TEMPLATE

Hello [name], we are selecting a small number of organisations to examine one bounded communication workflow with VENTEX Connect for 30 days. The pilot starts with approved test data, named stop criteria and a documented fallback channel. The aim is evidence about usability, device change and operational coordination - not a certificate. Would a 20-minute fit call with [role] be useful?

PERSONALISE

- Name one concrete workflow
- Make no unsupported security claim
- Record recipient, role and legitimate context
- Respect opt-out; never mass mail

09

Outreach email – after the call

Subject: Pilot scope, protection boundary and next decision

TEMPLATE

Thank you for the call. We identified [workflow] with [cohort] as a possible scope. [Data/processes] remain excluded. Before launch we confirm the Pilot Owner, permitted data, fallback channel, success criteria and stop criteria. The charter and playbook are attached. If those points fit, we propose a 60-minute kick-off in the week beginning [date].

ATTACHMENTS

- Pilot Launch Kit
- Secure Communication Pilot Playbook
- Product and security boundaries
- Security reporting contact

10

Weekly operating rhythm

The pilot needs little meeting time but a fixed cadence for friction, risk and decisions.

MONDAY

Confirm the target workflow and blockers. Scope changes require written approval.

WEDNESDAY

15-minute operator check: what was slow, unclear, unsafe or bypassed?

FRIDAY

Update the Evidence Matrix, classify events and name the next hypothesis.

11

Evidence Matrix

An entry is defensible only when observation and artefact remain separate.

COLUMNS

- ID and date
- Hypothesis or requirement
- Observed workflow
- Metric or result
- Artefact/link
- Owner
- Rating: met / partial / unmet / not tested

EXAMPLE

EV-07 | revoke lost device | test device removed | old session rejected after 42 s | redacted event record | Security Contact | met

NO ARTEFACT = NO PUBLIC CLAIM

12

Interview guide

Interview roles separately. Start open; the moderator must not defend the product.

OPERATOR

- What job were you trying to complete?
- Where did you hesitate or use a workaround?
- What information was missing at decision time?
- What felt secure, and why?
- What would you refuse to use tomorrow?

IT AND SECURITY

- Were device and session states understandable?
- Which revocation or recovery task was unclear?
- Which records are missing for approval?
- Which assumption should be tested next?

13

Final report

The report separates fact, interpretation and decision. Internal release does not require a marketing case study.

STRUCTURE

1. scope and protection boundary
2. cohort and dates
3. workflows tested
4. Evidence Matrix and incidents
5. results per success criterion
6. open risks
7. recommendation with conditions

DECISION

- GO - bounded expansion with conditions
- ITERATE - another pilot after named changes
- STOP - insufficient benefit, security or operability
- NO DECISION - incomplete evidence

14

Anonymised case study

Publication is optional and requires separate approval. The organisation, people and operating details are named only with explicit consent.

RELEASE STRUCTURE

- Situation without identifying details
- Bounded pilot scope
- Observed outcomes and measurement method
- Friction and unmet criteria
- Changes after the pilot
- Release owner and date

EDITORIAL CHECK

- No logos without brand permission
- No implied certification
- No relative percentage without denominator
- No security claim based on self-report alone

15

Pilot close-out

Before closure, access, data, open issues and publication rights are reconciled.

CLOSE-OUT

- Export participant and device inventory
- Revoke sessions no longer needed
- Delete or transition pilot data as agreed
- Close open security events
- Approve the final report
- Record case-study consent separately

OWNER DECISION

Decision: _____ Conditions: _____ Owner: _____ Date: _____

16

Primary sources and limits

The method is informed by recognised primary sources but makes no compliance or certification claim.

SOURCES

- NIST SP 800-61 Rev. 3 - Incident Response Recommendations
- NIST SP 800-63B-4 - Authentication and Authenticator Lifecycle
- CISA - Emergency Communications Guidance
- EU GDPR - Regulation (EU) 2016/679
- RFC 9420 - The Messaging Layer Security Protocol

URLS

csrc.nist.gov/pubs/sp/800/61/r3/final
pages.nist.gov/800-63-4/sp800-63b/
cisa.gov/emergency-communications-guidance-documents-and-publications
eur-lex.europa.eu/eli/reg/2016/679/oj
datatracker.ietf.org/doc/html/rfc9420

VERSION 1.0 / REVIEW 13 AUGUST 2026 / legal@ventex-connect.com