

Implementation & Change Management Playbook

A practical guide to help teams deploy Island in the public sector, enable secure access to priority apps, and drive adoption without slowing mission delivery.





What is *Island*?

Island is an enterprise browser that delivers a familiar browsing experience while embedding security controls directly into the browser. This helps public sector organizations reduce the day-to-day friction that often comes with legacy access patterns, without relying on heavy “rip and replace” projects.

Who This Playbook Is For

- IT and endpoint operations leading deployment and support
- Security defining guardrails for sensitive workflows
- Program and business leaders coordinating users, timelines, and adoption

What You Will Achieve

- Deliver secure, seamless access to web and SaaS applications.
- Reduce exposure to phishing and unsafe browsing behaviors.
- Onboard third-party contractors quickly with clear guardrails.
- Support BYOD scenarios while maintaining control over sensitive actions.

How to Deliver Immediate *Impact*

The fastest way to create value is to start with one high-friction workflow, a clearly defined pilot cohort, and a small set of controls that reduce risk without getting in the way.

Choose one impact wedge:



Third-Party or Contractor Access

- **Best when:** the organization needs surge staffing, vendors, or integrators to be productive quickly.
- **Why it works:** clear boundary (specific users, specific apps), fast to measure time-to-work.



A Single Sensitive SaaS Workflow

- **Best when:** a web app contains operational, citizen, student, patient, or mission-sensitive data.
- **Why it works:** easy to define what “safe handling” means (download, copy/paste, printing).



Reduce VDI Dependence for Browser-Based Work

- **Best when:** VDI is being used primarily for web apps, and the user experience is a persistent pain point.
- **Why it works:** immediate user-perceived performance improvement, visible reduction in tickets.

What to Expect

Many public sector teams can reach first measurable value in a few weeks, depending on approvals, identity readiness, and the complexity of the initial workflow.

Pilot Blueprint

(What “good” looks like)

In this playbook, a pilot is the first structured stage of adoption. It can be a proof of concept (PoC), a limited initial deployment tied to a small purchase, or the first rollout phase after an organization has already purchased Island. Regardless of the commercial path, the goal is the same: prove value quickly with a defined workflow, a defined cohort, and measurable outcomes.

A pilot succeeds when it is narrow, measurable, and easy to support.

Recommended Pilot Scope

Cohort Size	25–250 users (smaller is fine if the workflow is high value)
Apps	1–3 primary apps
Controls	3–6 core controls tied to the workflow’s risk profile
Timeline	2–6 weeks end-to-end for a first pass (varies by approvals and identity)

Define Success Metrics

Pick 2-3 metrics that are easy to pull and easy to defend.

Time-to-work for
new users or
contractors
(days)

Support tickets
tied to
VDI/VPN/remote
access (count)

Reduction in
VDI usage for
browser-based
workflows
(rough %)

Optional: pilot
adoption (active
users / eligible
users)

Pre-Launch Checklist (Phase 0)

Use this section to align owners and eliminate the most common deployment blockers.

Owners (name the people, not the departments)

IT Owner	Accountable for deployment and endpoint operations
Security Owner	Accountable for policy decisions and exception handling
Program Owner	Accountable for user readiness and communications
Helpdesk Lead	Accountable for frontline support and escalation

Readiness Checklist

☐ Confirm identity approach (SSO/MFA) and who owns it

☐ Identify the apps and workflows in scope

☐ Confirm the pilot cohort and enrollment method

☐ Agree on support paths and escalation contacts

Deliverable: a one-page pilot charter (template included below)

Deployment Runbook (Phase 1)

This is the step-by-step sequence most teams can follow.

Step 1: Prepare the Pilot Cohort

- ☐ Confirm the roster (names, roles, locations)

- ☐ Confirm device scenarios (managed devices, unmanaged devices, mixed)

- ☐ Confirm where users will be working (on-site, remote)

Step 2: Deploy Island

- ☐ Choose the deployment method that fits your environment (managed deployment for agency devices, guided install for BYOD or contractors where appropriate)

- ☐ Validate installation with a simple “go/no-go” check:
 - User can sign in
 - User can reach the in-scope app
 - User can complete one core workflow step end-to-end

Step 3: Enable secure access to in-scope apps

- ☐ Start with the minimum set of apps needed for the workflow

- ☐ Validate:
 - Authentication and session handling
 - Basic performance and usability
 - Supportability (helpdesk can reproduce and triage issues)

Step 4: Apply the minimum viable control set

Controls should be tied to the workflow's data sensitivity and the most likely failure modes.

Common controls (use what fits):

- Download restrictions for sensitive workflows
- Copy/paste boundaries to prevent data leakage
- Print controls for regulated content
- Session controls (timeouts, re-authentication where appropriate)

Rule of thumb: if a control makes the workflow unusable, it will be worked around. Tune until the secure workflow is the easiest workflow.

Step 5: Validate with a short test script

Have 5–10 pilot users complete:

- Normal login
- One standard workflow (the primary task users are expected to complete)
 - Example: Sign in → open the in-scope app → complete a core action (submit a case update, approve a request, upload a document, or enter a record).
- One policy edge case (a common “what if” moment that should be controlled for sensitive work)
 - Example: Attempt to copy text from the app into another destination.
 - Example: Attempt to download a file from the app.
 - Example: Attempt to print a record.
- A help request submission (so support flow is tested before you scale)

Step 6: Operate for two weeks, then hold a retro

In the retro, decide one of three paths:

- Expand cohort
- Adjust controls
- Change the initial workflow (if you picked the wrong wedge)

Security Guidance

This section is designed for security leaders who need clarity without jargon.

What “last-mile control” means:

Most policy failures happen at the moment a user interacts with data in an application. “Last-mile control” means the organization can enforce guardrails at the point of interaction, such as restricting copying sensitive text into unmanaged locations, or limiting downloads and prints for specific workflows.

Start conservative, then tune:

- Begin with a small cohort and the narrowest app list that still produces measurable value.
- Use a small control set that is easy to explain and audit.
- Create an exception path for urgent mission needs.

How Island Fits With Existing Security Programs

Island is typically used to complement identity and security controls by adding a managed workspace layer where most work happens today: the browser.

Change Management & Adoption

Adoption is easiest when the experience is familiar and the “why” is clear.

Message to users (simple and consistent)

- Island is a familiar browser experience.
- The goal is to reduce friction while keeping sensitive work safe.
- Some actions may be restricted for specific workflows (download, copy/paste, print).

Operating Model

(Support & Escalation)

Tiered Support Model

Helpdesk	Install issues, basic access, known issue
Identity Team	SSO/MFA, account provisioning, authentication errors
Security	Policy blocks, exception requests, control tuning
App owner / IT	Application access issues not related to identity

What to Capture in Tickets

- ☐ User + cohort
- ☐ Device type and where they are working (on-site, remote)
- ☐ App and workflow step
- ☐ Error message or screenshot
- ☐ Time of incident

Measurement & Reporting

Use a simple weekly check-in until you scale beyond the pilot.

Weekly pilot metrics (recommended)

☐

New users onboarded (count)

☐

Time-to-work for new users (days)

☐

VDI/VPN-related tickets for the pilot cohort (count)

☐

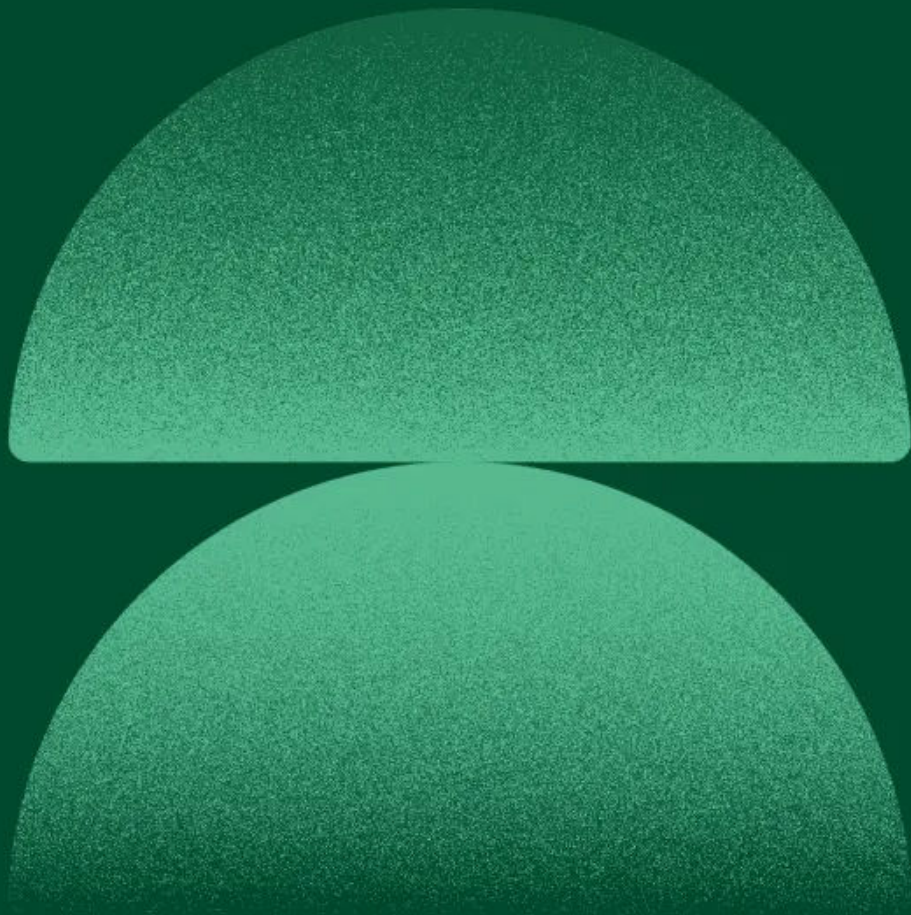
One qualitative signal: “What got easier this week?”

Decision Thresholds

- If adoption is low because of confusion: improve comms + quick start.
- If adoption is low because controls block core work: tune controls.
- If value is unclear: pick a different wedge with a clearer metric.



Change Management Templates



Pilot Charter

Pilot name:

Impact wedge (choose one): Contractor access / Sensitive SaaS workflow / VDI reduction for browser-based work

Workflow in scope:

Cohort:

- Who:
- Size:
- Locations (if relevant):
- Devices (managed, unmanaged, mixed):

In-scope apps (1-3):

-
-

Control set (v1):

- Downloads:
- Copy/paste:
- Print:
- Session handling:

Success metrics (choose 2-3):

-
-
-

Out of scope (v1):

-
-

Owners:

- IT owner:
- Security owner:
- Program owner:
- Helpdesk lead:

Support and escalation:

- Helpdesk:
- Identity:
- Security:
- Escalation contact:

Timeline:

- Kickoff:
- Cohort live:
- Retro:

Sample Email to Send Your Team

Subject: A faster, safer way to access [app/workflow]

Hi team,

Starting [date], [group/cohort] will use Island to access [apps/workflow]. Island is an enterprise browser that looks and works like a familiar browser experience, while adding safety controls in the background.

What changes

- Use Island for [apps/workflow].
- Depending on the workflow, certain actions may be limited (download, copy/paste, print).

What does not change

- Your day-to-day workflow stays the same.
- The goal is to reduce friction while keeping sensitive work safe.

Need help?

Contact [helpdesk contact] and mention “Island pilot.”

Thanks,
[signature]

Helpdesk Triage Note

Capture in the ticket

- User name + cohort
- Device type and location (on-site, remote)
- App and workflow step
- What happened (error text or screenshot)
- Time of issue

Route the ticket

- Install / launch issue → Helpdesk
- Login/SSO/MFA/account issue → Identity owner
- Policy blocked action (download/copy/print) → Security owner
- App-specific access issue → App owner / IT + Identity if auth-related

Escalation

If a mission-critical workflow is blocked, escalate to [name/role] within [SLA].

FAQs

What is Island?

Island is a secure enterprise browser used for specific work applications. It looks and feels like a familiar browser experience, with safety controls operating in the background.

What do I need to do differently?

Use Island for the apps and workflows included in your pilot or rollout. For everything else, follow your organization's normal guidance.

Will this slow me down?

Most users experience a familiar workflow with fewer "extra steps." Some actions may be limited in sensitive workflows to protect data. Overall, this should actually make work more efficient while also keeping us more secure.

What actions might be restricted, and why?

Depending on the workflow, Island may limit:

- Downloading files
- Copying and pasting text or data
- Printing

These controls help prevent sensitive information from being saved or shared in unapproved ways.

I tried to download, copy/paste, or print and it was blocked.**What should I do?**

If the action is needed for your work:

- Contact [helpdesk contact]
- Include the app name, what you were trying to do, and the message you saw (a screenshot helps)

Can I still use my usual device or work remotely?

Your department will provide guidance for your rollout. In many programs, Island supports flexible access patterns, including remote work and BYOD scenarios, while keeping controls in place for sensitive workflows.

Final Rollout Checklist

- ☐ Select an impact wedge and define the workflow

- ☐ Name owners (IT, Security, Program, Helpdesk)

- ☐ Confirm cohort and enrollment method

- ☐ Confirm app list (in scope / out of scope)

- ☐ Choose 2–3 success metrics

- ☐ Deploy Island to cohort

- ☐ Validate workflow end-to-end

- ☐ Apply minimum viable controls

- ☐ Operate for two weeks and review metrics

- ☐ Decide: expand cohort, tune controls, or change wedge

Explore how
Island is
supporting the
public sector.