

DEEP INFOSEC / PUBLIC GUIDE

Sovereign & Connected Infrastructure

Secure data centres, connected facilities, critical-service continuity and local operational ownership.

Engineering, security and operating capability — brought together around the outcome your organisation needs.

deepinfosec.com • sales.general@deepinfosec.com

What this means for your organisation

Understand how technical architecture, reliable communications, backup, access control and maintainability fit together.

Sovereign digital solutions

Digital sovereignty becomes meaningful when the organization controls its information, dependencies and options. We design architectures around data residence, customer-managed keys, supplier interoperability, privileged access and recoverability. The goal is practical independence: the ability to operate, investigate, migrate and improve critical systems with a clear understanding of each external dependency.

Managed data centres

A managed data-centre service must remain reliable when applications change, links fail and teams rotate. We design hosting, segmentation, access, backup, recovery and operational reporting around the criticality of each workload. Infrastructure supplied for managed services is ISO-certified within the applicable provider scope, while customer ownership, data residency and exit arrangements are built into the architecture.

IoT & connected systems

A connected device is part of an operational chain, not an isolated sensor. We design device identity, trusted communication, edge processing, firmware lifecycle, secure integration and maintenance around the actual use case. Whether the deployment serves a campus, fleet or utility network, the customer needs both useful data and a manageable device estate years after installation.

Industrial OT security

Industrial cybersecurity cannot disrupt the process it is meant to protect. We map safety-critical assets, maintenance windows, control-network dependencies and recovery conditions before recommending segmentation, monitoring or access changes. The engineering package gives operations and security teams a common, site-specific plan that can be tested and handed over.

Workstreams and outputs

Sovereign digital solutions

Architecture design, controlled digitisation, engineering and managed operation; proprietary components are distinguished from open export formats and documented integrations.

- Sovereign architecture: select data control, identity, cryptography, key custody, jurisdiction and deployment patterns for public agencies and regulated operators.
- Secure digitalisation: plan capture, metadata, indexing, preservation and controlled access for historical archives, records, research and institutional knowledge.

What you receive: Sovereignty and data-flow decision matrix

Managed data centres

Managed hosting, hybrid infrastructure or design/build support; facilities, certified provider scopes and availability commitments are defined in the client contract.

- Sovereign hosting architecture: design site, rack, compute, network, storage, identity and encryption domains around jurisdiction and data-residency requirements.
- Managed infrastructure: provision and operate approved virtualized, hybrid or private-cloud services on ISO-certified infrastructure within the contracted certification scope.

What you receive: Hosting and residency architecture with responsibility boundaries

IoT & connected systems

Device design review, integration engineering or fleet-security operations; partner hardware and protocols are assessed within the engagement.

- Embedded and connected-product security: threat models, secure boot and firmware update strategy, device identity, signing keys and lifecycle protection.
- Edge and communication: gateway architecture, segmentation, secure protocols, local failover and resilience when cloud links are unavailable.

What you receive: Device threat model and secure-design control matrix

Industrial OT security

Assessment first, architecture next, implementation under operator change authority; IEC 62443 approaches used as appropriate to the specific installation.

- Industrial discovery: inventory PLCs, HMIs, historian, SCADA, engineering workstations, remote access and process dependencies through passive or site-approved methods.
- Secure zone architecture: design Purdue-aligned segmentation, conduits, gateways, maintenance access and monitoring, avoiding assumptions that office IT controls fit plant operations.

What you receive: OT/ICS asset and communication-zone inventory

A practical engagement, from first scope to handover

01 Define the decision

We agree what must change, which systems matter, what the organisation already owns and what constitutes an acceptable outcome.

02 Evaluate on the right perimeter

A scoped assessment or pilot gives engineering teams sufficient information to choose a realistic deployment and acceptance plan.

03 Deliver with evidence

The team delivers designs, implemented controls or services, records decisions, tests outcomes and explains operating responsibilities.

04 Transfer operational capability

Documentation, knowledge transfer, maintenance pathways and follow-up are part of a sustainable programme.

Talk directly to the specialist team

Explore the full offering at deepinfosec.com and select the specialty matching your objectives. Public introductions are freely available; confidential technical and commercial dossiers follow a controlled customer process.

deepinfosec.com · sales.general@deepinfosec.com