# Title: [enter descriptive title]

|  |  |
| --- | --- |
| Requested | Date: 07/02/2025 Name: |
| Reason / Justification | Enter a clear description of the key drivers for this implementation or change. |
| Policy/SOP Compliance | Enter a policy or SOP which will govern this change. |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Services / Applications | Scope | Duration |
| Business/Service Interruptions | [SYSTEM NAME] | [ALL USERS?] | 1-2 hours |

# Preparation

1. Capture SRVPRINT snapshot on vCenter prior to changes
2. Verify latest VM backup in
3. Download Infor Enterprise Connector installer on
4. Create local admin service account for use on the Enterprise Connector
   1. Grant required permissions (printer access, local admin)
5. Prepare a 10GB SQL DB on
   1. Needed for DB tables/stored procedures
   2. Create RO SQL login
6. Verify networking configuration
   1. Infor URLs: (Still awaiting full list)
   2. AWS URLs:
7. Validate prerequisites on
   1. Required windows features installed (.NET framework, etc.)
   2. AV exclusions configured on Defender for connector files and services

# Implementation and Cutover

1. Install Infor Enterprise Connector on
   1. Configure settings as outlined in
   2. Configure local admin svc account on connector
2. Configure SonicWall firewall rules to allow outbound HTTPS and required ports (443, 28089-28091) to Infor and AWS endpoints:
   1. AWS/Infor URLs (*Awaiting Infor URLs*)
3. Configure SQL database connection
   1. Use SQL account during installer setup

# Verification and Testing

1. Confirm installation is complete and service is active
   1. Expected value: “OK”
2. Endpoint Connectivity
   1. Validate outbound internet access to required Infor and AWS URLs.
   2. Test using Test-NetConnection
   3. Confirm DNS can resolve all Infor/AWS endpoints from SRVPRINT
3. Review connector logs for successful job processing and free of errors
4. Connect with CSI users and conduct printing tests of job packets

# Recovery from Failure

1. Uninstall the Infor Enterprise Connector from SRVPRINT.
2. Roll back any database changes made on SRVSQL related to the connector
3. Disable or remove the local service account created for the connector.
4. Temporary disable firewall rules before full removal
5. If more issues arise, revert SRVPRINT to snapshot captured in vCenter.
6. Worst case, restore from Veeam backup

# Post-implementation & Cleanup

1. Confirm all temporary installation files are removed from SRVPRINT
2. Document new configuration to reflect changes and gather support information
3. Remove VM snapshot after 1 week of issue-free functionality
4. Close the change request ticket once all validation is complete

# Change Management

|  |  |
| --- | --- |
| Approved by | Adan Lopez |
| Impact to Confidentiality | Risk factors and potential threats |
| Impact to Integrity |  |
| Impact to Availability |  |

|  |  |  |
| --- | --- | --- |
| Control | Examples | Addressed in the plan? |
| SC.L2-3.13.2 – Security Engineering: Below is a list of the engineering principles and architectural designs which are selected and employed when planning security architecture or architectural modifications to the information system. | | |
| AC.L2-3.1.1 – Authorized Access Control [CUI Data] | **List and Authorize** any data access, privileged access, service accounts | n/a |
| AC.L2-3.1.2 – Transaction & Function Control | Database, permissions, roles, read/write | n/a |
| AC.L2-3.1.3 – Control CUI Flow | CUI boundaries, ports, firewalls, interfaces | n/a |
| AC.L2-3.1.5 – Least Privilege | PAM, JIT, separate admin account, minimum priv | n/a |
| AC.L2-3.1.20 – External Connections [CUI Data | Cloud, FedRAMP, verified connections | n/a |
| AU.L2-3.3.5 – Audit Correlation | SIEM, log forwarding, review | n/a |
| CM.L2-3.4.7 – Nonessential Functionality | Baselines, features, functionality | n/a |
| IA.L2-3.5.3 – Multifactor Authentication | Strong auth, | n/a |
| IA.L2-3.5.10 – Cryptographically-Protected Passwords | Keeper, API Keys, secure transfer | n/a |
| MP.L2-3.8.9 – Protect Backups | Veeam job | n/a |
| CA.L2-3.12.3 – Security Control Monitoring | Add to Security Checklist Manual | n/a |
| CA.L2-3.12.4 – System Security Plan | Update SSP/Cyber Manual | n/a |
| SC.L2-3.13.1 – Boundary Protection [CUI Data] | Boundaries, ACL, firewalls, IDS | n/a |
| SC.L2-3.13.11 – CUI Encryption | Encryption/protocols | n/a |
| SI.L2-3.14.1 – Flaw Remediation [CUI Data | Patches, vulnerability | n/a |
| SI.L2-3.14.2 – Malicious Code Protection [CUI Data] | EDR agents | n/a |
| AT.L2-3.2.2 – Role-Based Training | JIT training video, article, AI-generated tutorial, quiz | n/a |
| SC.L2-3.13.2 – Security Engineering | Threat modeling, review diagram, pentest, best practice guide | Links to…  [Security Diagrams](file:///C:\Users\alopez\OneDrive%20-%20Kirkhill,%20Inc\_Compliance\SSP\Diagrams)  [Guide to a Secure Enterprise Network Landscape](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.pdf)  [Zero Trust Architecture](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf)  [Microsoft Azure Well-Architected Framework](https://learn.microsoft.com/en-us/azure/well-architected/) |

# Resources

Insert diagram below which illustrates how the implementation will be implemented in the context of the existing network environment.

Diagram, box and whisker chart

AI-generated content may be incorrect.