

**POWERLOCK NETWORK SECURITY
AUDIT PROGRAM**

Group Name	Audit Step Name	Objective	Guidance	Audit Step
Planning & Organization	Administration Review	Roles and Responsibilities for PowerLock Administration have been clearly and appropriately defined	<p>CONTROL</p> <p>CONSIDERATIONS:</p> <ol style="list-style-type: none"> 1. Standards and guidelines for maintaining adequate PowerLock security are documented. 2. Management should formally assign the responsibility for assuring both logical and physical security of the PowerLock to deal with overall security issues 	<ol style="list-style-type: none"> 1. Review PowerLock documentation to gain an understanding of the PowerLock's capabilities and limitations 2. Verify that the Computer Operational Manual (COM) contains standards and policies for maintaining a secure and administratively controlled PowerLock Location Security Rules, PowerLock User Security Rules and PowerLock Switch Profiles 3. Is there documentation that clearly defines the roles and responsibilities of PowerLock administration, including training and testing of PowerLock Configuration? 4. Is there a list of authorized PowerLock administrators? (Identify primary and backup administrators) 5. Determine who is responsible for ensuring that the PowerLock security rules and configuration is in compliance with COM 6. Verify that local management is aware of these control requirements.
Acquisition & Implementation	Access Control	Adequate controls are in place over the configuration of user profiles, and user access rights are commensurate	<p>CONTROL</p> <p>CONSIDERATIONS:</p> <ol style="list-style-type: none"> 1. A control processing in place to review and confirm access rights 	<ol style="list-style-type: none"> 1. Is there a process used to authorize employees and non-employees access (add, change, delete) to the AS/400 2. What level of access are privileges granted

**POWERLOCK NETWORK SECURITY
AUDIT PROGRAM**

Group Name	Audit Step Name	Objective	Guidance	Audit Step
		with the user's job responsibilities. Access to PowerLock commands, tools and utilities is reliably to only authorized users	periodically for all AS/400 systems 2. Users are assigned system access that is commensurate with their job responsibilities 3. Access privileges are only assigned based on approved documentation	3. Are there controls that ensure that access to the AS/400 and PowerLock administration is granted to only those authorized individuals 4. Obtain a list of users with access to the PowerLock administration and reconcile to documented requests. Is each user uniquely identifiable? 5. Select a sample of remote users to confirm that they are set-up according with their needs and belong to the proper supplemental group
Delivery & Support	Configuration	Existing PowerLock security parameters are configured to secure settings and these settings are in compliance with corporate best practices and standards	Control Considerations: 1. Formal Policies and standards are available to guide in the process for administering & Configuring PowerLock 2. A control in place to review and confirm membership & Supplemental groups rules defined for all production systems	1. Verify that the COM contains a formal set of group membership rules defined and is controlled by the authorities defined over the supplemental groups 2. Obtain a list of the Supplemental Groups. Review the Client Function, server function and access permissions extended to these groups; compare to the standard security rules defined in COM. 3. What are the PowerLock Security rules currently in place 4. Is the PowerLock configured according to COM Standards and Guidelines?
Delivery & Support	Change Controls	All changes (i.e. Additions, deletions, etc) to the PowerLock configuration settings are reliably documented and	Control Considerations: 1. All changes are supported by authorized request from the user department 2. Independent post-	1. Is there a PowerLock change control procedure in place? i. Is there documentation for all PowerLock configuration changes ii. Have all of the changes been

**POWERLOCK NETWORK SECURITY
AUDIT PROGRAM**

Group Name	Audit Step Name	Objective	Guidance	Audit Step
		authorized	<p>implementation reviews are performed for all changes applied to PowerLock Configuration rules and access privileges</p> <p>3. A change control management system defined</p>	<p>authorized</p> <p>2. Assess the adequacy of the approval process</p>
Monitoring	PowerLock is monitored on a Periodic basis	Appropriate security events are logged to provide security administration personnel with the ability to appropriately monitor system security and appropriate reports are produced to summarize data recorded in audit logs so that security events may be efficiently monitored on a timely basis	<p>Control Considerations:</p> <p>1. The use of FTP, Telnet and ODBC services in any AS/400 networked environment are strictly controlled</p> <p>2. The PowerLock Network Security is configured to recognize and generate alert for any access violations</p>	<p>1. What are the exceptions which response has been defined</p> <p>2. Obtain a copy of PowerLock reports for review</p> <p>3. In discussion with the system administrator determine the process for monitoring and reporting on access violations to client functions and OS/400 Server. Also determine if changes (authorized and unauthorized) to the PowerLock configuration & rules are monitored and reported.</p> <p>4. Determine the process for reviewing the exception reports generated by PowerLock and verify that there is evidence of appropriate follow up by management</p> <p>5. Are the PowerLock reports adequate in providing management with necessary information to help analyze PowerLock activities (client/server function & authority for a user or group, user</p>

**POWERLOCK NETWORK SECURITY
AUDIT PROGRAM**

Group Name	Audit Step Name	Objective	Guidance	Audit Step
				<p>excluded from access, record unauthorized access attempts, etc)</p> <p>6. Determine what security is in place over the log files that contain any exception information</p> <p>7. Verify that the FTP and Telnet user privileges defined on any AS/400 environment are authorized and controlled</p>