



# PowerLock & ISO 17799 Standards

## Summary

---

### PowerLock & ISO 17799 Compliance

ISO 17799 is a comprehensive set of controls comprising best practices in information security. It's essentially an internationally recognized generic information security standard. In this paper, PowerTech describes how its tools and applications can help organizations comply or adhere to security standards related to AS/400 systems.

The following outlines ten prime sections that comprise the standard and where PowerLock can be leveraged:

- **Security Policy**  
[PowerLock Network Security, PowerLock Security Audit](#)
- **Security Organization**  
[PowerLock Network Security](#)
- **Asset classification and Control**  
[PowerLock Network Security](#)
- **Personnel Security**
- **Physical and Environmental Security**  
[PowerLock Network Security](#)
- **Communications & Operations Management**  
[PowerLock Network Security, PowerLock Security Audit](#)
- **System Access Control**  
[PowerLock Network Security, PowerLock Security Audit](#)
- **System Development and Maintenance**  
[PowerLock Network Security](#)
- **Business Continuity Planning**
- **Compliance**  
[PowerLock Network Security, PowerLock Security Audit](#)

We have addressed those sections and specific areas of the standards where our applications can help customers achieve compliance on **AS/400 systems**...

## PowerLock Details

---

### 3 Security policy

#### 3.1 Information security policy

Objective: To provide management direction and support for information security. Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

PowerLock SecurityAudit and NetworkSecurity have specific reporting features that enable detailed auditing such that policies can be constructed based on information gathered. Reports can be set to run on a scheduled basis consistent with corporate security policies.

d) a definition of general and specific responsibilities for information security management, including reporting security incidents;

PowerLock SecurityAudit helps define the process for reporting security events and provide data defined by the policies. PowerLock NetworkSecurity can send security information to third party consoles such as RealSecure SiteProtector from Internet Security Systems (ISS).

### 4 Organizational security

#### 4.2 Security of third party access

Objective: To maintain the security of organizational information processing facilities and information assets accessed by third parties. Access to the organization's information processing facilities by third parties should be controlled.

Where there is a business need for such third party access, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in a contract with the third party. Third party access may also involve other participants. Contracts conferring third party access should include allowance for designation of other eligible participants and conditions for their access. This standard could be used as a basis for such contracts and when considering the outsourcing of information processing.

PowerLock NetworkSecurity was specifically designed to precisely control and audit network access from any PC or device to the AS/400 system through common network services like FTP, ODBC, Telnet, and Remote Command.

#### 4.2.1.1 Types of access

The type of access given to a third party is of special importance. For example, the risks of access across a network connection are different from risks resulting from physical access. Types of access that should be considered are:

- a) physical access, e.g. to offices, computer rooms, filing cabinets;
- b) logical access, e.g. to an organization's databases, information systems.

PC and device access to the AS/400 system can be controlled by user, group, or IP address utilizing PowerLock NetworkSecurity. This application controls what and how data is access by third party through network connections such as ODBC, FTP, and File Transfer.

To further enhance asset protection PowerLock can be configured to monitor third party activity (24/7) and audit all activity through the AS/400 system.

## 5 Asset classification and control

### 5.2 Information classification

Objective: To ensure that information assets receive an appropriate level of protection. Information should be classified to indicate the need, priorities and degree of protection. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification system should be used to define an appropriate set of protection levels, and communicate the need for special handling measures.

PowerLock NetworkSecurity allows for varying degrees of access control, ensuring that network transactions from PCs are consistent with information classification policy. Without NetworkSecurity, users may have access to data on the AS/400 through the network, even though the data is protected using menu level security.

#### 5.2.1 Classification guidelines

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, and the business impacts associated with such needs, e.g. unauthorized access or damage to the information. In general, the classification given to information is a shorthand way of determining how this information is to be handled and protected.

PowerLock NetworkSecurity can help enforce classification guidelines on the AS/400 by restricting access to data. Access rules can be enforced for users, groups of users, or IP address locations.

## 7 Physical and environmental security

### 7.3.1 Clear desk and clear screen policy

Organizations should consider adopting a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities in order to reduce the risks of unauthorized access, loss of, and damage to information during and outside normal working hours. The policy should take into account the information security classifications (see 5.2), the corresponding risks and cultural aspects of the organization.

c) Personal computers and computer terminals and printers should not be left logged on when unattended and should be protected by key locks, passwords or other controls when not in use.

PowerLock NetworkSecurity application allows security administrators to control when and how AS/400 sessions can be inactivated. If PC systems are inactive for a limited amount of time, administrative criteria will command the AS/400 to defend itself by timing out and ending jobs, disconnecting jobs, or messaging the session with a warning. Separately, PowerLock NetworkSecurity can also send a notification to an administrator's message queue for other action.

## 8 Communications and operations management

### 8.1.3 Incident management procedures

Incident management responsibilities and procedures should be established to ensure a quick, effective and orderly response to security incidents (see also 6.3.1). The following controls should be considered.

- a) Procedures should be established to cover all potential types of security incident, including:
- 1) information system failures and loss of service;
  - 2) denial of service;
  - 3) errors resulting from incomplete or inaccurate business data;
  - 4) breaches of confidentiality.

PowerLock NetworkSecurity enables AS/400 Administrators to execute procedures that audit, detect, and respond to AS/400 network security incidents. PowerLock Interact can be configured to send AS/400 security events to the RealSecure SiteProtector security management console from ISS.

PowerLock SecurityAudit enables Administrators to detect and report on AS/400 system failures due to system over-load such as data and disk space storage.

- c) Audit trails and similar evidence should be collected (see 12.1.7) and secured, as appropriate, for:
- 1) internal problem analysis;
  - 2) use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;

With PowerLock NetworkSecurity all network traffic to and from the AS/400 system can be stored and logged in secure journals on the system creating a complete audit trail of activity that is eligible to be used for criminal proceedings or in the court of law. SecurityAudit enables quick retrieval of AS/400 database information for all audit functions.

- d) Action to recover from security breaches and correct system failures should be carefully and formally controlled. The procedures should ensure that:
- 1) only clearly identified and authorized staff are allowed access to live systems and data (see also 4.2.2 for third party access);
  - 2) all emergency actions taken are documented in detail;
  - 3) emergency action is reported to management and reviewed in an orderly manner;
  - 4) the integrity of business systems and controls is confirmed with minimal delay.

PowerLock NetworkSecurity enables administrators to precisely control who has access to AS/400 systems via the network through ODBC, FTP, etc. Administrators can also control access to the security application controls and administrative rights.

PowerLock applications can help to quickly validate object changes and network breaches on the AS/400 system.

### 8.2.1 Capacity planning

Capacity demands should be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available. These projections should take account of new business and system requirements and current and projected trends in the organization's information processing.

The StorageSensor feature in PowerLock SecurityAudit enables AS/400 system administrators to monitor and report on disk and data storage capacity to ensure system and performance integrity.

## 8.4 Housekeeping

Objective: To maintain the integrity and availability of information processing and

communication services. Routine procedures should be established for carrying out the agreed back-up strategy (see 11.1) taking back-up copies of data and rehearsing their timely restoration, logging events and faults and, where appropriate, monitoring the equipment environment.

b) Back-up information should be given an appropriate level of physical and environmental protection (see clause 7) consistent with the standards applied at the main site. The controls applied to media at the main site should be extended to cover the back-up site.

PowerLock NetworkSecurity supports disaster recovery and high availability environments by enabling precise control of network access rules on the backup AS/400 system. The backup system can contain two sets of access rules: one set for back up mode; and another set for production operation. Both rules can be configured to be called automatically depending on how the system is used.

## 8.5 Network management

### 8.5.1 Network controls

A range of controls is required to achieve and maintain security in computer networks. Network managers should implement controls to ensure the security of data in networks, and the protection of connected services from unauthorized access. In particular, the following controls should be considered.

c) If necessary, special controls should be established to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems (see 9.4 and 10.3). Special controls may also be required to maintain the availability of the network services and computers connected.

PowerLock NetworkSecurity enables administrators to precisely control user access from and through public networks to the AS/400.

### 8.6.4 Security of system documentation

System documentation may contain a range of sensitive information, e.g. descriptions of applications processes, procedures, data structures, authorization processes (see also 9.1). The following controls should be considered to protect system documentation from unauthorized access.

- a) System documentation should be stored securely.
- b) The access list for system documentation should be kept to a minimum and authorized by the application owner.
- c) System documentation held on a public network, or supplied via a public network, should be appropriately protected.

PowerLock NetworkSecurity enables specific network access and can restrict anyone from documentation through the network.

### 8.7.3 Electronic commerce security

Electronic commerce can involve the use of electronic data interchange (EDI), electronic mail and on line transactions across public networks such as the Internet. Electronic commerce is vulnerable to a number of network threats which may result in fraudulent activity, contract dispute and disclosure or modification of information. Controls should be applied to protect electronic commerce from such threats. Security considerations for electronic commerce should include the following controls.

- a) Authentication. What level of confidence should the customer and trader require in each others claimed identity?
- b) Authorization. Who is authorized to set prices, issue or sign key trading documents? How does the trading partner know this?

PowerLock NetworkSecurity enables AS/400 administrators to carefully regulate how much access a user can have through the network and who can have this type of access to the AS/400. Access control rules can be defined by user, group, or IP address. NetworkSecurity controls what and how data is access by third party through network connections such as ODBC, FTP, and File Transfer.

## 9 Access control

### 9.1.1.1 Policy and business requirements

Business requirements for access control should be defined and documented. Access control rules and rights for each user or group of users should be clearly stated in an access policy statement. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The policy should take account of the following:

- d) consistency between the access control and information classification policies of different systems and networks;

PowerLock NetworkSecurity enables network access control to the AS/400 system to match that of other internal access controls throughout the IT infrastructure.

- f) standard user access profiles for common categories of job;

All network access by AS/400 users can be controlled and audited based on individual user job requirements or job responsibilities using PowerLock NetworkSecurity.

### 9.1.1.2 Access control rules

In specifying the access control rules, care should be taken to consider the following:

a) differentiating between rules that must always be enforced and rules that are optional or conditional;

PowerLock SecurityAudit can help administrators determine access control rules that are required for network access to the AS/400 system versus those that can be used for backup systems, etc.

b) establishing rules based on the premise “What must be generally forbidden unless expressly permitted” rather than the weaker rule “Everything is generally permitted unless expressly forbidden”;

Consistent with this policy, PowerTech recommends that new users should first audit their existing traffic before setting up access control rules, and then allow the known acceptable transactions before locking out all other network transactions.

d) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;

Network access by AS/400 users through the network can only be controlled by the administrator, unless users are provided with administration rights in PowerLock NetworkSecurity.

## 9.2 User access management

Objective: To prevent unauthorized access to information systems.

Formal procedures should be in place to control the allocation of access rights to information systems and services.

The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

PowerLock NetworkSecurity enables administrators to precisely control all network access by users to the AS/400 system (ODBC, FTP, File Transfer, etc.).

PowerLock AuthorityManager features can be used to grant privileged access rights (special authorities on the AS/400) to users only on a need to have basis.

### 9.2.2 Privilege management

The allocation and use of privileges (any feature or facility of a multi-user information system that enables the user to override system or application controls) should be restricted and controlled. Inappropriate use of system privileges is often found to be a major contributory factor to the failure of systems that have been breached.

All Network transactions such ODBC, FTP, File Transfers, etc. to the AS/400 by users can be control to maintain user privilege integrity through PowerLock.

PowerLock SecurityAudit includes reports on the use of adopted authorities, which is one method that privileges could be abused.

PowerLock AuthorityManager features can be used to grant privileged access rights (special authorities on the AS/400) to users only on a need to have basis.

### 9.2.4 Review of user access rights

To maintain effective control over access to data and information services, management should conduct a formal process at regular intervals to review users' access rights so that:

a) users' access rights are reviewed at regular intervals (a period of 6 months is recommended) and after any changes (see 9.2.1);

AS/400 and network user access can be checked regularly utilizing our PowerLock SecurityAudit tool. A series of standard reports exist for user profiles and their access rights (e.g. dormant users, users with command line capability, users with special authorities). Reports can be scheduled to run at regular intervals.

b) authorizations for special privileged access rights (see 9.2.2) should be reviewed at more frequent intervals; a period of 3 months is recommended;

Special authorities can be monitored and tracked by user on a regular basis utilizing our PowerLock SecurityAudit tool.

### 9.3.1 Password Use

Users should follow good security practices in the selection and use of passwords. Passwords provide a means of validating a user's identity and thus to establish access rights to information processing facilities or services. All users should be advised to:

- a) keep passwords confidential;
- b) avoid keeping a paper record of passwords, unless this can be stored securely;
- c) change passwords whenever there is any indication of possible system or password compromise;
- d) select quality passwords with a minimum length of six characters which are:

- e) change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;
- f) change temporary passwords at the first log-on;

PowerLock SecurityAudit provides a complete system value report that includes all the QPWD\* system values that set and control password policy on the AS/400. The product documentation explains the various password management settings and suggests appropriate values.

### 9.3.2 Unattended user equipment

Users should ensure that unattended equipment has appropriate protection. Equipment installed in user areas, e.g. workstations or file servers, may require specific protection from unauthorized access when left unattended for an extended period. All users and contractors should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

- a) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;
- b) log-off mainframe computers when the session is finished (i.e. not just switch off the PC or terminal);

PowerLock NetworkSecurity includes a SecureScreen features that allows security administrators to control when and how AS/400 sessions can be inactivated. If PC systems are inactive for a limited amount of time, administrative criteria will command the AS/400 to defend itself by timing out and ending jobs, disconnecting jobs, or messaging the session with a warning. Separately, PowerLock NetworkSecurity can also send a notification to an administrator's message queue for other action.

## 9.4 Network access control

Objective: Protection of networked services.

Access to both internal and external networked services should be controlled.

This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services by ensuring:

- a) appropriate interfaces between the organization's network and networks owned by other organizations, or public networks;

PowerLock NetworkSecurity provides ability to precisely control network access to the AS/400 through transactions such ODBC, FTP, and File Transfer.

c) control of user access to information services.

PowerLock NetworkSecurity provides ability to precisely control network access to the AS/400 through transactions such ODBC, FTP, and File Transfer. Access control can be applied to over 31 host services on the AS/400 system.

#### 9.4.7 Network connection control

Access control policy requirements for shared networks, especially those extending across organizational boundaries, may require the incorporation of controls to restrict the connection capability of the users. Such controls can be implemented through network gateways that filter traffic by means of pre-defined tables or rules. The restrictions applied should be based on the access policy and requirements of the business applications (see 9.1), and should be maintained and updated accordingly.

Examples of applications to which restrictions should be applied are:

- a) electronic mail;
- b) one-way file transfer;
- c) both-ways file transfer;
- d) interactive access;

AS/400 application access through the network ports such as SQL service, FTP service, etc can controlled by user, user groups, IP address, or groups of IP addresses.

#### 9.5 Operating system access control

Objective: To prevent unauthorized computer access.

Security facilities at the operating system level should be used to restrict access to computer resources. These facilities should be capable of the following:

- a) identifying and verifying the identity, and if necessary the terminal or location of each authorized user;
- b) recording successful and failed system accesses;

PowerLock SecurityAudit can track all AS/400 invalid login attempts by user or IP address.

#### 9.5.2 Terminal Logon Procedures

Access to information services should be attainable via a secure log-on process. The procedure for logging into a computer system should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with unnecessary assistance. A good log-on procedure should:

- a) not display system or application identifiers until the log-on process has been successfully completed;

- b) display a general notice warning that the computer should only be accessed by authorized users;
- c) not provide help messages during the log-on procedure that would aid an unauthorized user;
- d) validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;

The default OS/400 logon screen does not comply with this standard. PowerTech can suggest alternative screens that meet these requirements.

### 9.5.5 Use of system utilities

Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. It is essential that their use is restricted and tightly controlled.

Emulation utilities, such as Client Access, enable AS/400 user to view, extract, and alter data on the AS/400 through the network. PowerLock NetworkSecurity can be used to precisely control user access to AS/400 data via the network using these types of utilities.

The number of people with command line access on the AS/400 should be limited. PowerLock SecurityAudit can generate a list of users that have command line access.

PowerLock AuthorityManager features can be used to grant privileged access rights (special authorities on the AS/400) to users only on a need to have basis, thus restricting general access to system utilities from the command line.

### 9.7 Monitoring system access and use

Objective: To detect unauthorized activities.

Systems should be monitored to detect deviation from access control policy and record monitorable events to provide evidence in case of security incidents. System monitoring allows the effectiveness of controls adopted to be checked and conformity to an access policy model (see 9.1) to be verified.

PowerTech NetworkSecurity enables 24/7 real-time security monitoring through existing messaging products or through PowerTech's solutions.

#### 9.7.1 Event logging

Audit logs recording exceptions and other security-relevant events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

Audit logs should also include:

- a) user IDs;

- b) dates and times for log-on and log-off;
- c) terminal identity or location if possible;
- d) records of successful and rejected system access attempts;
- e) records of successful and rejected data and other resource access attempts.

[Yes, PowerLock NetworkSecurity includes all of the above information in its audit reports for network transactions on the AS/400.](#)

Certain audit logs may be required to be archived as part of the record retention policy or because of requirements to collect evidence (see also clause 12).

[AS/400 security / non-security related events and AS/400 network transactions can be audited and stored for use in subsequent investigations.](#)

#### 9.7.2.1 Procedures and areas of risk

Procedures for monitoring use of information processing facilities should be established. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities should be determined by a risk assessment. Areas that should be considered include:

a) authorized access, including detail such as:

1) the user ID;

[Yes, 24/7 real-time security monitoring \(PowerLock NetworkSecurity\)](#)

2) the date and time of key events;

[Yes, 24/7 real-time security monitoring \(PowerLock NetworkSecurity\)](#)

3) the types of events;

[Yes, 24/7 real-time security monitoring \(PowerLock NetworkSecurity\)](#)

4) the files accessed;

[Yes, 24/7 real-time security monitoring \(PowerLock NetworkSecurity\)](#)

5) the program/utilities used;

[Yes, 24/7 real-time security monitoring \(PowerLock NetworkSecurity\)](#)

b) all privileged operations, such as:

1) use of supervisor account;

[Yes, 24/7 real-time security monitoring \(PowerLock NetworkSecurity\)](#)

2) system start-up and stop;

Yes, using SecurityAudit

- 3) I/O device attachment/detachment;

Yes, using SecurityAudit

- c) unauthorized access attempts, such as:

- 1) failed attempts;

Yes, 24/7 real-time monitoring of network failed attempts; OS logon failed attempts.

- 2) access policy violations and notifications for network gateways and firewalls;

Yes, 24/7 real-time monitoring of all network access to the AS/400

- 3) alerts from proprietary intrusion detection systems;

PowerLock NetworkSecurity can send alerts and events to Internet Security Systems IDS console for enterprise integration.

- d) system alerts or failures such as:

- 1) console alerts or messages;

Yes, PowerLock can generate and send 24/7 real-time alerts to a GUI console. NetworkSecurity can integrate with most messaging products to provide the same type of functionality.

- 2) system log exceptions;

PowerLock SecurityAudit enables file integrity and exception reporting.

- 3) network management alarms.

PowerLock generates alarms for any network traffic entering the AS/400 system via host servers.

### 9.7.2.3 Logging and reviewing events

A log review involves understanding the threats faced by the system and the manner in which these may arise. Examples of events that might require further investigation in case of security incidents are given in 9.7.1.

System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation should be considered.

Yes, PowerLock SecurityAudit simplifies the task of reviewing data that has been stored in the Operating Systems' SecurityAuditJournal.

## 10 Systems development and maintenance

### 10.2 Security in application systems

Objective: To prevent loss, modification or misuse of user data in application systems. Appropriate controls and audit trails or activity logs should be designed into application systems, including user written applications. These should include the validation of input data, internal processing and output data.

PowerLock applications enable AS/400 application security by providing network controls to the applications and comprehensive auditing.

#### 10.2.2.1 Areas of risk

Data that has been correctly entered can be corrupted by processing errors or through deliberate acts. Validation checks should be incorporated into systems to detect such corruption. The design of applications should ensure that restrictions are implemented to minimize the risk of processing failures leading to a loss of integrity. Specific areas to consider include:

a) the use and location in programs of add and delete functions to implement changes to data;

PowerLock NetworkSecurity can be utilized to precisely control users from viewing, changing, adding, or deleting AS/400 data through network services.

### 10.4 Security of system files

Objective: To ensure that IT projects and support activities are conducted in a secure manner. Access to system files should be controlled.

PowerLock NetworkSecurity can be utilized to precisely control users from viewing, changing, adding, or deleting AS/400 data and system files through network services.

#### 10.4.3 Access control to program source library

In order to reduce the potential for corruption of computer programs; strict control should be maintained over access to program source libraries as follows (see also 8.3).

c) IT support staff should not have unrestricted access to program source libraries.

PowerLock NetworkSecurity can be used to block or control all user, regardless of special authorities or OS authority levels, network service access to the AS/400 system.

g) An audit log should be maintained of all accesses to program source libraries.

PowerLock applications can be used to track access to files and libraries on the AS/400 system.