

OS/400 SECURITY POLICY

Purpose: The purpose of this OS/400 Security Policy is to establish baseline security standards for the configuration of IBM server iSeries equipment. The implementation of this security policy will minimize unauthorized access to proprietary information and technology. *The policy is PowerTech copyrighted material. There is no charge for its usage. Copying, distribution, and modifications are covered by the terms of the license agreement at the back of this document.*

1.0 Physical Security

- ▶ The Computer system must be kept in a secure room or area with limited personnel access.
- ▶ The computer room doors must have locks that can record who accessed the computer room at a given date/time.
- ▶ The computer room should have limited, or no windows. If windows are present, there should be adequate barriers and/or alarms to prevent human access.
- ▶ A list of persons authorized to access the secured computer room must be maintained and periodically updated.
- ▶ Persons who are admitted to the computer room, but are not on the list of authorized persons, must be required to be signed in, escorted while present in, and signed out of the computer room.
- ▶ The Computer room must have adequate power, and Uninterruptible Power Supply (UPS) that will ensure continuous operations when power is unavailable. The UPS must provide adequate power for a period of not less than 10 minutes.
- ▶ A fire suppression system must be present that will prevent, or minimize harm to persons and equipment in the computer room in the event of a fire.

2.0 Data Recoverability

- ▶ The Data Recovery strategy must be tested no less often than annually.
- ▶ The entire system, including the operating system and utilities, must be backed up no less often than quarterly.
- ▶ Business applications must be backed up no less often than weekly.
- ▶ Data for business applications should be backed up no less often than daily.

- ▶ Data in database files must be journaled to ensure up to the second recoverability.
- ▶ Journal receivers should be backed up no less often than daily.
*Note: High Availability software and systems satisfy this requirement.
- ▶ Sensitive data must be encrypted before being written to tape.
- ▶ Encryption keys must not be stored on the same tape, or in the same receptacle as the encrypted data that can be unlocked with such keys.
- ▶ At least one version of the backed up data must be stored off site.
- ▶ Data moved off site must be transported in locked storage boxes.
- ▶ An inventory of the contents of every locked storage box should be kept in each subsequent locked storage box.

3.0 Data Access Security

- ▶ Only users with a demonstrated business need should be able to read or change data.
- ▶ IT staff must not have access to production data unless prior authorization is given. When IT staff need to access production data, all activity must be audited and reported. Activity reports must be kept on hand for not less than 6 months.
- ▶ Production data must not be replicated to any test environment without first cleaning and scrambling sensitive data. Sensitive data is defined as personally identifiable private information (including, but not limited to Drivers License Number, Credit Card Number, Passport Number, etc.), and company confidential information.
- ▶ Customer, or company, confidential information must not be copied from the system or removed from the premises without prior authorization.
- ▶ All attempts (successful or not) to copy data off of the system must be recorded in a secure journal. Reports from this journal must be reviewed regularly, and kept in archive for not less than 6 months.
- ▶ Sign-on security – The default signon display for an OS/400 telnet session must be modified as follows:
 - The default input capable fields of Menu, Program, and Library, must be modified so as not to allow user input at signon time.
 - The default error messages for Invalid Password, Invalid User, etc. must be modified to the simple statement "User Cannot Signon" so as not to provide clues as to the problem.

- A statement must be added that declares that the system is the private and proprietary property of the organization and access is only allowed through prior authorization.

4.0 User Profile Security

▶ 4.1 - Common User Profile parameters

These User Profile parameters must be set for all system users:

- The Text Description must identify the User, and their department.
- Display Signon Information must be set to either "Yes" (DSPSGNINF(*YES)), or to the System Value (DSPSGNINF(*SYSVAL)).
- Password Expiration Interval must be set to either "90" (PWDEXPITV(90)), or to the System Value (PWDEXPITV (*SYSVAL)).
- The public authority for the profile must be exclude (AUT(*EXCLUDE)).

▶ 4.2 - Non IT User Profile parameters

The User Profile parameters for a non IT User must be set as follows:

- User Class set to "User" (USRCLS(*USER)).
- Initial program must be a program name and a library name (not "*LIBL") that restricts the user to only the business applications needed for their job function (INLPGM(MyLib/MyPgm)).
- Initial menu set to signoff (INLMNU(*SIGNOFF)).
- The limited capability parameter set to "Yes" (LMTCPB(*YES)).
- Special Authority parameter set to none (SPCAUT(*NONE)).

▶ 4.3 - System Operator User Profile parameters

The User Profile parameters for a System Operator must be set as follows:

- User Class set to "User" (USRCLS(*SYSOPR)).
- Initial menu set to either the OS/400 main menu (INLMNU(MAIN)), or to another appropriate menu.
- The limited capability parameter set to "partial" (LMTCPB(*PARTIAL)).

▶ 4.4 - **Application Programmer User Profile parameters**

The User Profile parameters for an application programmer must be set as follows:

- User Class set to "Programmer" (USRCLS(*PGMR)).
- Initial menu set to either the OS/400 main menu (INLMNU(MAIN)), or to another appropriate menu.
- The limited capability parameter set to "partial" (LMTCPB(*PARTIAL)).
- Special Authority parameter set to none (SPCAUT(*JOBCTL)).
- Application Programmers that require more Special Authorities should receive those on a temporary, as needed basis.

▶ 4.5 - **System Administrator User Profile parameters**

The User Profile parameters for a System Administrator must be set as follows:

- User Class set to "Security Officer" (USRCLS(*SECOFR)).
- Initial menu set to either the OS/400 main menu (INLMNU(MAIN)), or to another appropriate menu.
- The limited capability parameter set to "partial" (LMTCPB(*PARTIAL)).
- Special Authority parameter set to none (SPCAUT(*JOBCTL *AUDIT)).
- Application Programmers that require more Special Authorities should receive those on a temporary, as needed basis.

▶ 4.6 - **Powerful User ID's**

- A roster must be kept of each User Profile that has powerful capabilities. A powerful user is defined as a profile that has one or more of the OS/400 special authorities, or one who has the ability to make direct updates to production data without using an approved application interface.
- User's whose profiles have one or more OS/400 special authorities (*ALLOBJ, *SECADM, etc.) must have specific authorization to those special authorities by their management.
- The use of profiles with OS/400 special authorities should be limited to strict operational need. During the times that a special authority is not

required, the user should not be carrying it in their active profile, but instead operate under a profile without special authorities.

- Users with any of *ALLOBJ, *IOSYSCFG, *SAVSYS, or *SECADM, special authority must have User Profile Auditing (CHGUSRAUD) turned on at all times.
- A log of activity for each session used by a powerful user must be produced and reviewed for appropriate actions.

▶ 4.7 - Group Profiles

- Group Profiles must have a password of *NONE.
- Group Profiles must not own application objects.
- Group Profiles must have a text description that clearly marks the profile as a Group Profile.

▶ 4.8 - IBM Supplied User Profiles

- IBM Profiles must not be used as a Group Profile for any user.
- IBM profiles must not own any objects created by users on this system. **Exception: The QSECOFR profile must be the owner of all other User Profiles.**
- No user should have more than *EXCLUDE rights to any IBM supplied User Profile object.
- The following IBM supplied User Profiles must have a password of *NONE, and only be given a password when an authorized use of the profile is required:

QSYSOPR	QPGMR	QUSER	QSRV
QSRVBAS	QBRMS	QSRVBAS	QBRMS
QDESADM	QDESUSR	QEJB	QEJBSVR
QMGM	QMQMADM	QNETSPLF	QNETWARE
QNFSANON	QRJE	QTCM	QTIVOLI
QTIVROOT	QTIVUSER	QTMHHTTP1	QTMHHTTP
QTMPLPD	QUMB	QUSER	

▶ **4.9 - The QSECOFR Profile**

- The QSECOFR Profile must have its password kept in a sealed envelope in a secured container. All access must be signed in and out, and the password must be changed after each use.
- Persons who have authority to use, or grant use to the QSECOFR password are: (*See Appendix A.*)
- Use of the QSECOFR Profile is discouraged. In nearly every situation a facsimile of the QSECOFR Profile with all of the same OS/400 special authorities will satisfy the needs of the organization.

▶ **4.10 - Non IBM Supplied User Profiles**

- User Profiles supplied, or created by, other vendors must have a password of *NONE, and should only be given a password when an authorized use of the profile is required.
- Vendor supplied User Profiles must not be used as a group profile – especially if the vendor supplied profile owns application objects.

▶ **4.11 - Passwords**

- Passwords must be kept secret and not shared with other persons.
- No IT person should ever ask any user to disclose their password.
- No User should ever disclose their password to another user for any reason.
- No User Profile should ever have a default password – either where the password is equal to the User ID name, or the password is set to a published and/or known value.
- Initial passwords must be set by the User Provisioning Authority. These passwords should be randomly generated, and the user should be required to change the password upon first use.
- Passwords should contain a variety of characters including a mixture of lower and upper case letters, numbers, special characters, and blanks.
- Passwords should not be easily recognized names, dates, or native language words.
- Passwords must never be stored in programs, scripts, database files, stream files, data areas, message files, message queues, or any other receptacle that is subject to monitored viewing by anyone but the owner of the password.

- A Password should only be given to a profile if only one person is responsible for the profile's use.

▶ **4.12 - Changing Passwords**

- Passwords must be changed at least every 90 days.
- Any given password should be unique from any of the last 10 passwords used by the user.
- A password cannot be retrieved. If the user forgets their password, a new one must be created for them.
- If a user forgets their password, a new password must be set by the User Provisioning Authority. The password should be randomly generated, and should be changed upon first use.

▶ **4.13 - Dormant Users**

- Users that have not logged on the system in the last 60 days must be disabled.
- Users that have not logged on to the system in 120 days must be deleted.
- When a user is deleted, any objects owned by that user should be assigned to the profile "OLDOBJOWNER".
- A list of special purpose profiles that are exempt from these provisions must be maintained by the system management.
- Profiles that are exempt from these provisions must have a password of *NONE.

5.0 System Configuration

- ▶ OS/400 System Values must be set, and maintained in these settings.
- ▶ OS/400 System Values must be reviewed not less frequently than weekly to determine their state of compliance.

► OS/400 System Values must be set as follows:

QALWOBJRST	*NONE
QALWUSRDMN	Shall not contain the values *ALL or *DIR
QAUDCTL	*AUDLVL, *OBJAUD, *NOQTEMP
QAUDENDACN	*NOTIFY
QAUDFRCLVL	*SYS
QAUDLVL	*AUTFAIL *DELETE *OBJMGT *SYSMGT *SAVRST *SECURITY *SERVICE *PGMFAIL
QAUDLVL2	Use QAUDLVL system value to set *SECURITY
QAUTOCFG	0
QAUTORMT	0
QAUTOVRT	100
QCMNRCYLMT	No recommendation
QCRTAUT	*EXCLUDE
QCRTOBJAUD	*NONE
QDEVRCYACN	*DSCMSG
QDSCJOBITV	120
QDSPSGNINF	1
QFRCCVNRST	No recommendation
QINACTIV	30
QINACTMSGQ	*DSCJOB
QMAXSGNACN	2
QMAXSIGN	5
QPWDEXPITV	90
QPWDLMTAJC	1
QPWDLMTCHR	*NONE
QPWDLMTREP	2
QPWDLVL	3
QPWDMAXLEN	128
QPWDMINLEN	6
QPWDPOSDIF	0
QPWDRQDDGT	1
QPWDRQDDIF	5
QPWDVLDPGM	*NONE
QRETSVRSEC	0
QRMTIPL	0
QRMTSIGN	*VERIFY
QRMTSRVATR	No recommendation
QSECURITY	40
QSHRMEMCTL	1
QUSEADPAUT	An authorization list
QVFOBJRST	3 or 5

6.0 Network Configuration Settings

- ▶ Network Configuration settings must be set, and maintained in these settings, as follows:

DDMACC	*REGFAC
JOBACN	*REJECT
PCSACC	*REGFAC

- ▶ The Following Registered Exit Programs must be set as follows:

QIBM_QHQ_DTAQ	DTAQ0100	POWERLOCK/PLKR107R
QIBM_QLZP_LICENSE	LICM0100	POWERLOCK/PLKR107R
QIBM_QMF_MESSAGE	MESS0100	POWERLOCK/PLKR107R
QIBM_QNPS_ENTRY	ENTR0100	POWERLOCK/PLKR107P
QIBM_QNPS_SPLF	SPLF0100	POWERLOCK/PLKR107P
QIBM_QPWFS_FILE_SERV	PWFS0100	POWERLOCK/PLKR107F
QIBM_QRQ_SQL	RSQL0100	POWERLOCK/PLKR107R
QIBM_QSQ_CLI_CONNECT	CLIC0100	POWERLOCK/PLKR107CLI
QIBM_QTF_TRANSFER	TRAN0100	POWERLOCK/PLKR107R
QIBM_QTG_DEVINIT	INIT0100	POWERLOCK/PLKR107TI
QIBM_QTMF_CLIENT_REQ	VLRQ0100	POWERLOCK/PLKR107FTP
QIBM_QTMF_SERVER_REQ	VLRQ0100	POWERLOCK/PLKR107FTP
QIBM_QTMF_SVR_LOGON	TCPL0100	POWERLOCK/PLKR107TS1
QIBM_QTMX_SERVER_REQ	VLRQ0100	POWERLOCK/PLKR107FTP
QIBM_QTMX_SVR_LOGON	TCPL0100	POWERLOCK/PLKR107TS1
QIBM_QTOD_SERVER_REQ	VLRQ0100	POWERLOCK/PLKR107TFT
QIBM_QVP_PRINTERS	PRNT0100	POWERLOCK/PLKR107R
QIBM_QZDA_INIT	ZDAI0100	POWERLOCK/PLKR107P
QIBM_QZDA_NDB1	ZDAD0100	POWERLOCK/PLKR107P
QIBM_QZDA_NDB1	ZDAD0200	POWERLOCK/PLKR107P
QIBM_QZDA_ROI1	ZDAR0100	POWERLOCK/PLKR107P
QIBM_QZDA_ROI1	ZDAR0200	POWERLOCK/PLKR107P
QIBM_QZDA_SQL1	ZDAQ0100	POWERLOCK/PLKR107P
QIBM_QZDA_SQL2	ZDAQ0200	POWERLOCK/PLKR107PS
QIBM_QZHQ_DATA_QUEUE	ZHQ00100	POWERLOCK/PLKR107P
QIBM_QZRC_RMT	CZRC0100	POWERLOCK/PLKR107P
QIBM_QZSC_LM	ZSCL0100	POWERLOCK/PLKR107P
QIBM_QZSC_NLS	ZSCN0100	POWERLOCK/PLKR107P
QIBM_QZSC_SM	ZSCS0100	POWERLOCK/PLKR107P
QIBM_QZSO_SIGNONSRV	ZSOY0100	POWERLOCK/PLKR107P

7.0 Library Authority

- ▶ All Libraries
 - All libraries must be secured against *PUBLIC access.
 - All libraries must have the public authority parameter (AUT) set to either *EXCLUDE, or to a named authorization list.
 - All libraries must have the Default public authority parameter (CRTAUT) set to *EXCLUDE.
 - All libraries must have the Default Object Auditing parameter (CRTOBJAUD) set to either *USRPRF.
 - Only those users who have a demonstrated business need to access a library should have rights to the library.
 - Users rights to any library should be no higher than *USE.
- ▶ Production Application Libraries
 - Production application libraries must be set as TYPE(*PROD).
- ▶ Test Libraries
 - Test libraries must be set as TYPE(*TEST).

8.0 Auditing

- ▶ The OS/400 Security Audit Journal (QAUDJRN) must be enabled at all times that the system is running.
- ▶ Security Audit Journal receivers must be retained for at least 6 months.
- ▶ The Audit Level System Values shall be set according to the System Values section of this document.
- ▶ User Auditing must be turned on for every Powerful User on the system.

9.0 Additional Topics for Future Consideration

- ▶ Out Queue Security
- ▶ Job Queue Security
- ▶ Monitoring of Database Changes
- ▶ Authorities to Sensitive Programs
- ▶ Virus Protection
- ▶ Encryption
 - For Sensitive Information on Disk
 - For Backup Tapes
 - For Transmitted Data
- ▶ Data Classification Policy
- ▶ PTF Level Policy
- ▶ Object Level Security for Files
- ▶ Object Level Security for Programs
- ▶ Programs and Jobs that adopt authority

APPENDIX A

▶ The QSECOFR Profile

- Record the Persons who have authority to use, or grant use to the QSECOFR password in the space provided below:



► **License Agreement**

This PowerTech Security Policy is provided to you free of charge, but is still protected by Copyright law. Your use of this Policy is subject to the terms and conditions below:

1. Give us credit! You may copy and distribute this Policy provided you conspicuously publish a copyright notice (© 2006 The PowerTech Group, Inc.) and always include the disclaimer of warranty and the part where we warn you that we're not going to be liable for the consequences of anyone using the recommendations in this Policy (it keeps us out of hot water). You also have to include a complete copy of this License and the warranty disclaimer in any copy you distribute to anybody else. Oh, and one more thing, we provided this Policy to you free of charge, so you can't go charging other people for access to and/or use of this Policy.

2. You may modify any portion of the policy and distribute this new version as long as you don't violate the terms of Section 1, and you agree to all of these conditions we're about to layout:

- If you change the policy, you have to take credit for (or own up to) your changes with a prominent notice stating what changed, and when.
- If you distribute or publish any part of this Policy, or you derive a new policy from it, you have to license the new work(s) for free too. It doesn't matter who you send it to, you can't charge them a fee for the Policy.
- Pay attention to this part because it is real important. If you change the Policy, you have to send a copy of your modifications to PowerTech at policy@powertech.com and you grant PowerTech a worldwide, royalty-free irrevocable, perpetual license to use, modify, and distribute your modifications as part of the Policy. We'll have a look at your submission and decide if we want to include it in a future release of the policy. No we're not going to pay you for it, but yes we will give you named credit as a contributor (unless you ask us to keep your identity anonymous). Heck, isn't that what Open Source is all about?

3. You don't have to accept this License, heck you haven't signed anything. It doesn't even affect you if you're just reading the policy. However, nothing else grants you permission to copy, distribute or modify the Policy. By definition if you copy, distribute, modify, or derive works from the Policy, you have accepted the License and all of its terms.

4. This policy is licensed free of charge, so naturally there is no warranty expressed or implied. If you are considering using this policy, then we'll assume you are an experienced OS/400 professional and therefore are experienced and intelligent enough to test any potential impacts of the policy before you implement any recommendations. You make up your own mind as to whether the recommendations in this policy are right for your systems. If you use this policy or its recommendations, you agree that we are not liable for any problems or damage you may do to your system. If you can't accept these conditions, don't use the policy.