IBM i SECURITY POLICY

Purpose: The purpose of this IBM i Security Policy is to establish baseline security standards for the configuration of Power Systems running IBM i (System i, iSeries, AS/400). Implementing this security policy can help you minimize unauthorized access to proprietary information and technology. *This policy is copyrighted material of PowerTech. There is no charge for its use. Copying, distribution, and modification issues are covered in the terms of the license agreement at the back of this document.*

1.0 Physical Security

- Keep the computer system in a secure room, or in an area with limited personnel access.
- The computer room doors must have locks that can record who accessed the computer room on any given date and time.
- The computer room should have a limited number of windows, or no windows. If there are windows, you should have adequate barriers or alarms to prevent human access.
- Maintain a list of the people authorized to access the secured computer room and keep it updated.
- Anyone who is not on the list of authorized computer room users must sign in to enter the computer room, be escorted while in the room, and must sign out when they leave.
- The computer room must have adequate power and an uninterruptible power supply (UPS) to ensure continuous operations if regular power is unavailable. The UPS must provide adequate power for at least 10 minutes.
- The computer room must have a fire suppression system to minimize harm to people and damage to equipment in the event of a fire.

2.0 Data Recoverability

- Test the data recovery strategy at least annually.
- Back up the entire system, including the operating system and software utilities, quarterly.
- Back up business applications at least weekly.
- Back up data for business applications daily.
- Journal the data in database files to ensure up-to-the-second recoverability.
- Back up journal receivers daily.
  Note: *High Availability (HA) software and systems satisfy this requirement.*
- Encrypt all sensitive data being written to tape.
- Do not store the encryption keys on the same tape or in the same receptacle as the encrypted data that can be unlocked with those keys.
- Store at least one version of backed-up data off-site.

TEL USA: 253.872.7788
TOLL FREE: 800.915.7700

- Transport all data moved off-site in locked storage boxes.
- Keep a copy of the inventory of the contents of each locked storage box in a different locked box and keep a master inventory list of the contents of all locked boxes.

3.0 Data Access Security

- Only users with a demonstrated business need should be authorized to read or change data.
- IT staff must not have access to production data without authorization. When IT staff needs access to production data, all of their activity must be audited and reported. Keep these activity reports at least 6 months.
- Do not replicate production data to any test environment without cleaning and scrambling sensitive data. Sensitive data is defined as personally identifiable private information (such as drivers license numbers, credit card numbers, and passport numbers) and confidential company information.
- Confidential information must not be copied from a system or removed from the premises without authorization.
- Record all attempts (successful or otherwise) to copy data from the system in a secure journal. Review the reports from this journal regularly and archive them for at least 6 months.
- Sign-on security: Modify the default sign-on display for an IBM i Telnet session as follows:
  - Modify the input-capable fields of Menu, Program, and Library so they don't allow user input at sign-on time.
  - Reword the default error messages for Invalid Password, Invalid User, and so forth, to "User Cannot Sign On" to avoid providing clues to the problem.
  - Add a statement that declares that the system is the private and proprietary property of the organization and that access is allowed only through prior authorization.

4.0 User Profile Security

- **4.1 – Common User Profile Parameters**
  Set these user profile parameters for all system users as follows:
  - The text description must identify the user and their department.
  - Set Display Signon Information to either "Yes" (DSPSGNINF(*YES)), or to the System Value (DSPSGNINF(*SYSVAL)).
  - Set Password Expiration Interval 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**
  Set the User Profile parameters for a non-IT user as follows:
  - Set the User Class to "User," (USRCLS(*USER)).
  - The Initial Program must be a program name and a library name (not "*LIBL") that restricts the user to only the business applications they need for their job: (INLPGM(MyLib/MyPgm)).
  - Set the Initial Menu to "Signoff," (INLMNU(*SIGNOFF)).
  - Set the Limit capabilities parameter to "Yes," (LMTCPB(*YES)).
  - Set the Special Authority parameter to "None," (SPCAUT(*NONE)).
- **4.3 – System Operator User Profile Parameters**
  Set the User Profile parameters for a system operator as follows:
  - Set the User Class to "System Operator," (USRCLS(*SYSOPR)).
  - Set the Initial Menu to either the IBM i Main Menu (INLMNU(MAIN)), or to another appropriate menu.
  - Set the Limit capabilities parameter to "Partial," (LMTCPB(*PARTIAL)).
- **4.4 – Application Programmer User Profile Parameters**
  Set the user profile parameters for an application programmer as follows:
  - Set the User Class to "Programmer," (USRCLS(*PGMR)).
  - Set the initial menu to either the IBM i Main Menu (INLMNU(MAIN)), or to another appropriate menu.
  - Set the Limit capabilities parameter to "Partial," (LMTCPB(*PARTIAL)).
  - Set the Special Authority parameter to "None," (SPCAUT(*JOBCTL)).
  - Any application programmers that need more special authorities should receive those on a temporary, as-needed basis.
- **4.5 – System Administrator User Profile Parameters**
  Set the User Profile parameters for a system administrator as follows:
  - Set the User Class to "Security Officer," (USRCLS(*SECOFR)).
  - Set the Initial Menu to either the IBM i Main Menu (INLMNU(MAIN)), or to another appropriate menu.
  - Set the Limit capabilities parameter to "Partial," (LMTCPB(*PARTIAL)).
  - Set the Special Authority parameter to "None," (SPCAUT(*JOBCTL *AUDIT)).
  - Any application programmers that need more special authorities should receive those on a temporary, as-needed basis.

- **4.6 – Powerful User IDs**
  Keep a roster of every powerful user profile. A powerful user profile is defined as any profile that has one or more IBM i special authorities, or has the ability to make direct updates to production data without using an approved application interface.
  - Users whose profiles have one or more IBM i special authorities (*ALLOBJ, *SECADM, and so forth) must have specific management authorization to those special authorities.
  - Limit the use of profiles with IBM i special authorities to operational need. During the times that a special authority is not required, the user should not have it in their active profile. They should operate under a profile without special authorities.
  - Users with *ALLOBJ, *IOSYSCFG, *SAVSYS, or *SECADM special authority must have User Profile Auditing (CHGUSRAUD) turned on at all times.
  - Produce a log of activity for each session of a powerful user and review it.
- **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 indicates the profile is a group profile.
- **4.8 – IBM-Supplied User Profiles**
  - Do not use IBM profiles as a group profile for any user.
  - IBM profiles must not own any objects created by users on the 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. They should be given a password only for authorized use of the profile:

QSYSOPR	QPGMR	QUSER	QSRV
QSRVBAS	QBRMS	QSRVBAS	QBRMS
QDESADM	QDESUSR	QEJB	QEJBSVR
QMGM	QMQMADM	QNETSPLF	QNETWARE
QNFSANON	QRJE	QTCM	QTIVOLI
QTIVROOT	QTIVUSER	QTMHHTP1	QTMHHTTP
QTMPLPD	QUMB	QUSER	

- **4.9 – The QSECOFR Profile**
  - Keep the QSECOFR profile password in a sealed envelope, in a secured container. Record all access to the password and have users sign in and out. Change the password after each use.
  - See Appendix A for a list of the people who have the authority to use, or grant use to, the QSECOFR password.
  - Avoid using the QSECOFR profile. In nearly every situation, a copy of the QSECOFR profile with the same IBM i special authorities will satisfy the organization's needs.
- **4.10 – Non-IBM-Supplied User Profiles**
  - User profiles that are supplied or created by other vendors must have a password of *NONE. Give these profiles a password only when an authorized use of the profile is required.
  - Do not use vendor-supplied user profiles as a group profile, especially if the vendor-supplied profile owns application objects.
- **4.11 – Passwords**
  - Keep passwords secret and do not share them with others.
  - No IT person should ever ask a user to reveal 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 or known value.
  - The User Provisioning Authority should set initial passwords. These passwords should be generated randomly and the user should be required to change the password on first use.
  - Passwords should contain a variety of characters, including a mixture of lowercase and uppercase letters, numbers, special characters, and blanks.
  - Passwords should not be easily recognized names, dates, or native language words.
  - Never store passwords in programs, scripts, database files, stream files, data areas, message files, message queues, or any receptacle that is subject to monitored viewing by anyone besides the owner of the password.
  - Give a password to a profile only if just one person is responsible for the profile's use.

- **4.12 – Changing Passwords**
  - Change passwords at least every 90 days.
  - A new password should be different from the last 10 of the user's passwords.
  - A password cannot be retrieved. If a user forgets their password, create a new password for the user.
  - If a user forgets their password, the User Provisioning Authority should set up a new, randomly generated password. The user should change this password on first use.
- **4.13 – Dormant Users**
  - Disable all users that have not logged on to the system in the last 60 days.
  - Delete all users that have not logged on to the system in the last 120 days.
  - When a user is deleted, assign any objects owned by that user to the OLDOBJOWNR profile.

  System management maintains a list of special purpose profiles that are exempt from these provisions. Any profiles that are exempt from these provisions must have a password of *NONE.

5.0 System Configuration

- Review IBM i system values weekly to determine their state of compliance.
- Set and maintain IBM i system values using the following policy:

Value	Policy Settings
QALWOBJRST	*NONE
QALWUSRDMN	Shall not contain the values *ALL or *DIR
QAUDCTL	*AUDLVL,*OBJAUD, *NOQTEMP
QAUDENDACN	*NOTIFY
QAUDFRCLVL	*SYS
QAUDLVL	*AUDLVL2 *AUTFAIL *DELETE *OBJMGT *SYSMGT *SAVRST *SECURITY *SERVICE *PGMFAIL
QAUDLVL2	*AUTFAIL *DELETE *OBJMGT *SYSMGT *SAVRST *SECURITY *SERVICE *PGMFAIL
QAUTOCFG	0
QAUTORMT	0
QAUTOVRT	100
QCMNRCYLMT	No recommendation
QCRTAUT	*EXCLUDE
QCRTOBJAUD	*NONE
QDEVRCYACN	*DSCMSG
QDSCJOBITV	120
QDSPSGNINF	1
QFRCCVNRST	No recommendation
QINACTITV	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

Value	Policy Settings
QPWDRQDDIF	5
QPWDVLDPGM	*NONE
QRETSVRSEC	0
QRMTIPL	0
QRMTSIGN	*VERIFY
QRMTSRVATR	No recommendation
QSECURITY	40
QSHRMEMCTL	1
QUSEADPAUT	An authorization list
QVFYOBJRST	3 or 5

6.0 Network Configuration Settings

- Set and maintain network configuration settings as follows:

Value	Setting
DDMACC	PTNS0107
JOBACN	*REJECT (unless still using SNADS)
PCSACC	*REGFAC

- Set these registered exit programs as follows:

Exit Program	Value	Setting
QIBM_QHQ_DTAQ	DTAQ0100	QGPL/PTNS0107
QIBM_QLZP_LICENSE	LICM0100	QGPL/PTNS0107
QIBM_QMF_MESSAGE	MESS0100	QGPL/PTNS0107
QIBM_QNPS_ENTRY	ENTR0100	QGPL/PTNS0107
QIBM_QNPS_SPLF	SPLF0100	QGPL/PTNS0107
QIBM_QPWFS_FILE_SERV	PWFS0100	QGPL/PTNS0107
QIBM_QRQ_SQL	RSQL0100	QGPL/PTNS0107
QIBM_QSQ_CLI_CONNECT	CLIC0100	QGPL/PTNS0107
QIBM_QTF_TRANSFER	TRAN0100	QGPL/PTNS0107
QIBM_QTG_DEVINIT	INIT0100	QGPL/PTNS0107
QIBM_QTMF_CLIENT_REQ	VLRQ0100	QGPL/PTNS0107
QIBM_QTMF_SERVER_REQ	VLRQ0100	QGPL/PTNS0107
QIBM_QTMF_SVR_LOGON	TCPL0100	QGPL/PTNS0107
QIBM_QTMX_SERVER_REQ	VLRQ0100	QGPL/PTNS0107
QIBM_QTMX_SVR_LOGON	TCPL0100	QGPL/PTNS0107
QIBM_QTOD_SERVER_REQ	VLRQ0100	QGPL/PTNS0107
QIBM_QVP_PRINTERS	PRNT0100	QGPL/PTNS0107
QIBM_QZDA_INIT	ZDAI0100	QGPL/PTNS0107
QIBM_QZDA_NDB1	ZDAD0100	QGPL/PTNS0107
QIBM_QZDA_NDB1	ZDAD0200	QGPL/PTNS0107
QIBM_QZDA_ROI1	ZDAR0100	QGPL/PTNS0107
QIBM_QZDA_ROI1	ZDAR0200	QGPL/PTNS0107
QIBM_QZDA_SQL1	ZDAQ0100	QGPL/PTNS0107
QIBM_QZDA_SQL2	ZDAQ0200	QGPL/PTNS0107
QIBM_QZHQ_DATA_QUEUE	ZHQ00100	QGPL/PTNS0107
QIBM_QZRC_RMT	CZRC0100	QGPL/PTNS0107
QIBM_QZSC_LM	ZSCL0100	QGPL/PTNS0107
QIBM_QZSC_NLS	ZSCN0100	QGPL/PTNS0107
QIBM_QZSC_SM	ZSCS0100	QGPL/PTNS0107
QIBM_QZSO_SIGNONSRV	ZSOY0100	QGPL/PTNS0107

7.0 Library Authority

- All Libraries
  - Secure all libraries against *PUBLIC access.
  - Set the Public Authority parameter (AUT) for all libraries to either *EXCLUDE, or to a named authorization list.
  - Set the Default Public Authority parameter (CRTAUT) for all libraries to *EXCLUDE.
  - Set the Default Object Auditing parameter (CRTOBJAUD) for all libraries to *USRPRF.
  - Only users with 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
  - Set production application libraries as TYPE(*PROD).
- Test Libraries
  - Set test libraries as TYPE(*TEST).

8.0 Auditing

- Enable the IBM i Security Audit Journal (QAUDJRN) any time the system is running.
- Retain Security Audit Journal receivers for at least 6 months.
- Set the QAUDLVL and QAUDLVL2 system values according to the System Configuration section in this document.
- Turn on User Auditing for every powerful user on the system.

9.0 Other Topics for Consideration

- Output queue security
- Job queue security
- Monitoring database changes
- Authorities to sensitive programs
- Virus protection
- Encryption
  - Sensitive information on disk
  - Backup tapes
  - 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

  In the space below, list everyone who has authority to use, or grant use to, the QSECOFR password:

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 (© 2011 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 have to include a complete copy of this license and the warranty disclaimer in any copy you distribute to anybody else. One more thing—we provided this policy to you free of charge, so you can't charge 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 lay out:

   - 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. No matter who you send it to, you can't charge them a fee for the policy.
   - Pay attention to this part because it's 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 Power-Tech 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). Isn't that what Open Source is all about?

3. You don't have to accept this license—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 there is no warranty, expressed or implied. If you are considering using this policy, we assume you're an experienced IBM i professional and are intelligent enough to test any potential impacts of the policy before you implement any recommendations. You must 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 PowerTech is 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.