



3000 Landerholm Circle SE • Bellevue, WA 98007-6484 • www.bellevuecollege.edu

IT Security Standard:

Database Management

Introduction

This standard defines the steps implementing the Bellevue College IT Security Policy with regard to the database management generally and the management of the database systems in use on campus specifically. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard addresses specific procedural and configuration elements for database management within the database systems currently deployed at Bellevue College: HP TurboImage and Microsoft SQL Server. However, database management also includes responsibility for the data stored and manipulated by these systems, and this standard is a companion to the Bellevue College IT security standard addressing “Data and Information Security.” All the requirements of that standard apply to database management operations on campus.

Exceptions

A variety of exceptions to this standard may be expected. These exceptions, when granted, will be documented in either a platform specific standard or in a memo documenting the exception. Exceptions may be granted by the Bellevue College IT Security Administrator, the Dean of Information Resources (IR), or any IR director authorized by the Dean. Copies of all documentation regarding exceptions will be kept on file with the Bellevue College IT Security Administrator. This documentation will include:

1. A detailed description of the exception.
2. A description of why the exception is necessary.
3. A risk assessment by the Bellevue College IT Security Administrator and/or the Dean of Information Resources, or designee.
4. A description of the compensating controls that are in place to mitigate risk created by the exception.

Business Impact and Risk, Threat, and Vulnerability Analysis

The data managed and stored by Bellevue College, both on-campus and off-campus in partnership with the Center for Information Resources (CIS), is most likely the college’s most valuable asset. Carefully administration of the hardware and software used to manage this data, thus protecting this data’s integrity and assuring its proper use are very important IT support tasks.

Given this importance of the database management systems, the most significant threats are:

1. Unauthorized disclosure for malicious purposes.
2. Unauthorized modification or destruction for malicious purposes.
3. Accidental modification or destruction during the course of assigned duties.
4. Accidental disclosure to unauthorized parties.

The risks associated with database management at Bellevue College are different, depending on the associated system being used to accomplish the task:

HP TurboImage:

Given the nature of the threat and the asset, the primary risks are not really associated with the database engine itself, but rather in the procedures for managing the data. The biggest risk is accidental disclosure, destruction or modification of data by IT support staff, a low vulnerability.

Microsoft SQL Server:

This product is extremely complex, highly network capable, and constantly changing, all of which contributes to a much higher level of vulnerability. Historically, the greatest risks associated with this database engine are unauthorized malicious attacks. These risks will be carefully assessed in each specific installation and carefully mitigated using updated standard practices.

Standard

A. Data Management

1. The management of data is an important function of those IR IT support personnel assigned to manage the databases used on campus, as well as the campus users with whom IR partners to accomplish this task. The data that is managed is broad in its nature and includes the college's business application data of which CIS is the custodian, as well as a tremendous amount of internal operational and procedural information.
2. The processes used by support personnel must ensure the data is only released following defined procedures, not inappropriately altered, and protected from disclosure. All data will be managed in accordance with the Bellevue College IT security standard addressing "Data and Information Security."

B. Database Systems

1. The roles of the Database Administrator (DBA) is defined by this standard as the person or group of people who have ultimate responsibility for the "care and feeding" of the database instance(s) installed on a Bellevue College computer system. With this responsibility comes a full administrative privilege to access each database. This database access does not assume permission for elevated administrative privileges at the computer or server's operating system level.
2. **HP TurboImage**

The following defines the CIS standard for creating and managing TurboImage databases on an HP3000 server. Typically, Bellevue College users utilize those databases created by the CIS.

 - a. The databases will be maintained and managed by authorized CIS staff in the Customer Services Department.
 - b. The manager login account of the computer system where the database resides will be defined as the creator of the database.
 - c. Structural changes to a database will be approved by the CIS application development lead in consultation with peers to assure the reliability and integrity of the applications and the data.
 - d. Structural changes to the database will be performed during the quarterly implementation processes, using procedures provided by the CIS Implementation Coordinator.
 - e. Database schemas may be left in the Program Library account after the implementation, but because they may contain passwords, they will be secured to assure they are not readable across accounts.
 - f. Each database will have a minimum of two passwords; one for read-write access used by the applications and another that provides read only access used for end-user reporting. Additional passwords will be defined to restrict access to specific tables or columns.
 - g. The read-write passwords will be changed quarterly with each general implementation. This password is known and used by authorized CIS and Bellevue College personnel, and maintained solely by CIS.
 - h. The read-only password is technically under Bellevue College's control, but will be changed quarterly also.

- i. All databases will be "secured" (as distinct from "released"). Exceptions will be documented.
- j. The Multi-processing Executive (MPE)/iX program Query will never be configured within the CIS application menu system on a production system.
- k. All connections to and users of the HP 3000 using TurboImage will be logged in accordance with CIS IT security standards.

3. Microsoft SQL Server

The following defines the Bellevue College standard for creating and managing a Microsoft SQL Server on a Windows server operating platform.

- a. All computers with Microsoft SQL Server installed will first be in compliance with the Bellevue College IT Security Standard addressing "Windows Base System Configuration."
- b. All the file and disk shares on the SQL Server computer must be read-only. Written exceptions will document the business purpose for any additional rights that are needed for any specific application or database and who has been granted those rights.
- c. The Bellevue College firewall will be configured to block all incoming access to the Microsoft SQL Server service ports (1433/tcp, 1434/tcp) from outside Bellevue College's network. If the service is configured to listen on non-default ports, those ports will also be blocked at the firewall.
- d. SQL Server will be installed with all unneeded components either removed (uninstalled) or disabled. All sample databases (i.e., pubs and northwind) will be removed. Guest users will be dropped from production databases.
- e. SQL Server will be installed to run as a non-privileged domain account, not as a local system. This account will be granted the one additional privilege of "login as service". The "optional privileges" of: network write, act as part of operating system, replace process level tokens, member of an administrators' local group, and/or member of local power users will not be granted.
- f. If any of the following registry keys exist for a particular installation, they and those keys contained within them will be restricted to allow access only from the Systems Administrator, the DBA, and the SQL Server user:
 - HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server
 - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSSQLServer
 - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSSQL\$InstanceName
 - HKEY_LOCAL_MACHINE\Software\Microsoft NT\CurrentVersion\Perflib
- g. Microsoft Windows NTFS permissions on the C:\Program Files\Microsoft SQL Server\MSSQL directory, and all files and directories it contains, will be configured to allow only the MS SQL Server account, DBA group, local system, and local and domain administrators full control. Other accounts will be granted no access.
- h. While antivirus software will be installed on the base computer system, it is recommended that the SQL Server database files be excluded from scans.
- i. SQL Server will be configured only on servers (as opposed to workstations) and will be managed by the Network Server Group. Servers on isolated and protected development networks may be managed by other technical support personnel, as assigned.
- j. Servers hosting SQL Server will be inside the firewall, not on the demilitarized zone (DMZ). Exceptions may be made for third-party products, but will be thoroughly documented and may require additional security to mitigate the additional risks.
- k. Servers hosting SQL Server will not provide Web services. Exceptions can be made for third-party products, but these will be thoroughly documented and may require additional security to mitigate the risks. Note: This does not apply to developmental/test installations located on the isolated development or test networks.

- l. A configured SQL Server using Windows authentication will be used when possible. If mixed mode authentication is used, the authentication will occur over an encrypted communications channel.
- m. The SQL Server System Administrator user and all other SQL Server logins will maintain complex passwords and be aged in compliance with the Bellevue College IT security standard addressing "Password Management."
- n. Domain user groups will be utilized to assign permissions on SQL Servers where possible. Individual domain user account access to servers will be limited to Database Administrators, Network Server Group administrators, and developers. Use of local user groups will be acceptable only if it is not possible to use domain groups. Access within servers and databases will be performed using pre-defined server roles wherever possible. DBA-defined user roles will be permissible where they are needed to more precisely limit user access.
- o. Login auditing at the SQL Server level will be enabled. The DBA will review error logs and event logs for security-related alerts and log-in failure daily.
- p. All structural changes and changes to user access rights for databases on production systems will be "logged" in a source version control system. This record of change history will be maintained for no less than one year.
- q. The Bellevue College DBA will be the only person(s) authorized to make structural changes to the databases on production systems.
- r. All data passed from the application layer will be validated prior to passing it to the database layer. These validations will include at a minimum: appropriate character classes (alphabetic, numeric, punctuation, white space, control) and minimum/maximum length edits. Other business rule edits will be done at the application layer or within the database if they are appropriate for the application design and are consistent with CIS development standards.
- s. SQL Server system administrators will be restricted to those authorized within Bellevue College.
- t. Consideration should be given to additional security within the database that might be appropriate for protecting confidential data, such as credit card numbers or a Personal Identification Number (PIN); this might include encryption of specific columns.
- u. The default system-stored procedures, including the extended stored procedures, will be configured to deny execute permission for all users except those in the sysadmin SQL Server fixed role. This is especially significant for the xp_cmdshell procedure.
- v. Data stored outside the SQL Server (e.g., backups, dumps, exports, replication files) will be secured with strict file system permissions allowing only minimum and authorized access. Any physical repositories of data outside the server (such as tapes, disks, etc.) will be secured from unauthorized access.
- w. Non-DBA users will be granted no access to the master tables, or views of those tables.
- x. Admin or user access for employees leaving the organization will be disabled no later than the day the person leaves employment.
- y. SQL Servers will not be linked. Exceptions will be granted and documented if needed for third party applications and cross-platform integration.
- z. Prevention of unauthorized access to linked servers will be by deleting the linked server entries that are no longer needed. Special attention will be paid to the login mapping between the local and remote servers. Logins with the bare minimum privileges for configuring linked servers will be used.

4. Microsoft SQL Server – Development

There are a few issues with Microsoft SQL Server that are of more keen interest to developers. These include:

- a. Messages from SQL Server will be sanitized prior to passing them back to the end-user; such things as paths, IP addresses, column names, table names, SQL commands, and login information will be removed.

- b. Bellevue College-created stored procedures will not be entered into the SQL Server master or msdb databases.
- c. The use of Open Database Connectivity (ODBC) and password management are addressed in the Bellevue College IT security standards addressing “Password Management” and “Application Development.”
- d. Persistent "temporary" table (i.e., those not maintained in memory) should be avoided. If they must be used, they will be configured with very limited access. Further, their contents will be removed as quickly as possible.
- e. Source code (e.g., schema, stored procedures) will be maintained, like all other developed applications, within a Bellevue College common software configuration management system.
- f. Unsupported or undocumented (e.g., hidden or internal) Application Program Interface (API) will not be used to manage and store data within the SQL Server database. Developers will be strongly encouraged to use only standard SQL API and not vendor proprietary extensions to the standard.
- g. Whenever possible, to centralize business logic within the database and allow for better control of the base tables, data manipulation by application programs will be performed through stored procedure wrappers instead of direct calls to the SQL verbs select, insert, update, and delete. User queries will be performed via view instead of the base tables.
- h. The sensitivity of particular data will be identified during application design and analysis, as well as in the creation of documentation and correspondence.

Sanctions

Violations of the provisions of this, or any Bellevue College IT security standard or policy, will be dealt with immediately in the same manner as any violations of Bellevue College policies, and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including:

1. Permanent loss of computer use privileges;
2. Denial of future access to Bellevue College IT resources;
3. Disciplinary action – any disciplinary action will be taken in accordance with appropriate procedures as established by the Vice President of Human Resources (for employees) or the Dean of Student Services (for students);
4. Dismissal from the college; and/or
5. Legal action.

Those users who misuse or abuse any computing or network resource may have their login accounts closed and access to the systems immediately terminated. Some violations of this standard may also constitute a state, local, or federal criminal offense.

Appendix A – References

1. Bellevue College IT Security Policy
2. Bellevue College IT Security Standard: Media Disposal
3. Bellevue College IT Security Standard: Password Management
4. Bellevue College IT Security Standard: Firewall Configuration and Change Management
5. Bellevue College IT Security Standard: Application Development
6. CIS IT Security Standard—CIS Data Management and Databases, January 29, 2003.
7. Killeen, LaMothe, Meinig, Smith, Holcomb; *Open Records & Open Meetings Deskbook*; <http://atg.wa.gov/records/deskbook.shtml>; 1998
8. Kondreddi, *Overview of SQL Server security model and security best practices*, http://vyaskn.tripod.com/sql_server_security_best_practices.htm, updated 2004
9. Litchfield, David; Advisories NSIR150002002B and NSIR190002002A <http://www.ngssoftware.com/advisory.htm>; 2002

10. Litchfield, David; *Threat Profiling Microsoft SQL Server (A Guide to Security Auditing)*; <http://www.ngssoftware.com/papers.htm>; 2002
11. *Microsoft SQL Server 2000 Operations Guide - Chapter 3 Security Administration*, <http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/sqlops0.mspx> , updated 2006
12. CERT; *CERT Incident Note IN-2002-04, Exploitation of Vulnerabilities in Microsoft SQL Server*; http://www.cert.org/incident_notes/IN-2002-04.html, 2002

Effective Date:	July 2003
Date Last Modified:	July 10.2009