



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

IT Security Standard:

byRequest Configuration

Introduction

This standard defines the specific steps needed to implementing Bellevue College policy # 5250: *Information Technology (IT) Security* regarding the byRequest product. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines specific procedural and configuration elements for use of byRequest to access print queues on the HP3000s located at Bellevue College. These procedural elements are in support of the IT Bellevue College Security Policy.

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, 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 (IR), 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 user account for accessing byRequest on the HP3000 will be configured with higher than normal operating system privileges. The account will have access to the colon (command shell) prompt and will be secured with a desktop password when left logged-in and unattended for extended periods.

Given these application requirements, the most significant threats are:

1. Malicious and/or unauthorized access to information.
2. Malicious, accidental, and/or unauthorized changes to, or deletion of, configuration or data.

Given the nature of the asset and the nature of the threat, the primary risk associated with the use of byRequest is the unauthorized access to data -- including student and employee data. This risk has additional potential risks associated with it of: loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work, and, to some degree, a loss of reputation.

Standard

A. Introduction

Hillary Software's product byRequest is used to manipulate the print queues on the HP3000 so that deferred printer requests are redirected from the HP3000 to an alternate output device. This alternate device may be a Web server, e-mail server, or a different print queue.

1. The byRequest product will be configured to use the WRQ pclick (software application created by WRQ - a software company) process for file transfers. The Telnet/FTP protocol options will not be used.
2. If byRequest is started and left running on an unattended workstation, that workstation will be located in a secured computer room facility.
3. The login to the HP3000 will use a unique session name and user name.
4. The byRequest account will be configured in MPE (HP3000 operating system) as follows:
 - a. An MPE password is not required, but a Security/3000 password is required.
 - b. Standard HP3000 password change and expiration procedures will apply to the user in accordance with the Bellevue College "Password Management" standard.
 - c. Capabilities of AM (Account Manager), ND (Input/Output Devices), SF (Permanent Files), IA (Interactive Access) will be configured for this login. The inactive session timeout will be disabled for this login if the physical access controls are accommodated.

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 Associate Dean of Student Success (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. *byRequest, Quick Reference Guide*, Hillary Software, Inc. 2002
2. SBCTC-IT Security Standard: *byRequest Configuration*
3. Bellevue College Policy #5250 – *Information Technology (IT) Security*
4. Bellevue College IT Security Standard: *Password Management*

Effective Date: July 2003
Date Last Modified: April 12, 2009