



All Applications Release Bulletin

April 2010

In this bulletin...

Redesigned Help Facility For My BackPack	2
New User Guides For My BackPack	3
Expanded User Name Field for My BackPack	3
Authorize.Net™ Gateway Support for My BackPack	4
Tracking Code Support For My BackPack	5
Simplified Word Processing User Preferences	6
Web User Mailing For Applicants and Parents	7
Senior Systems PCI Compliance Policy and WISP Document	10

About Release 91_7

This release incorporates new features and enhancements for **My BackPack**, including a re-designed help facility and some new user guides, an expanded User Name field to facilitate the use of email addresses for web IDs, support for the Authorize.Net™ payment gateway, and tracking code support for services such as Google Analytics™. In **System Administration**, there is also a new Web User Mailing function for applicants/parents. And, throughout the Senior Systems applications, the User Preferences for word processing have been simplified.

Also included in this bulletin are copies of Senior Systems documents related to PCI compliance and personal information security policies.

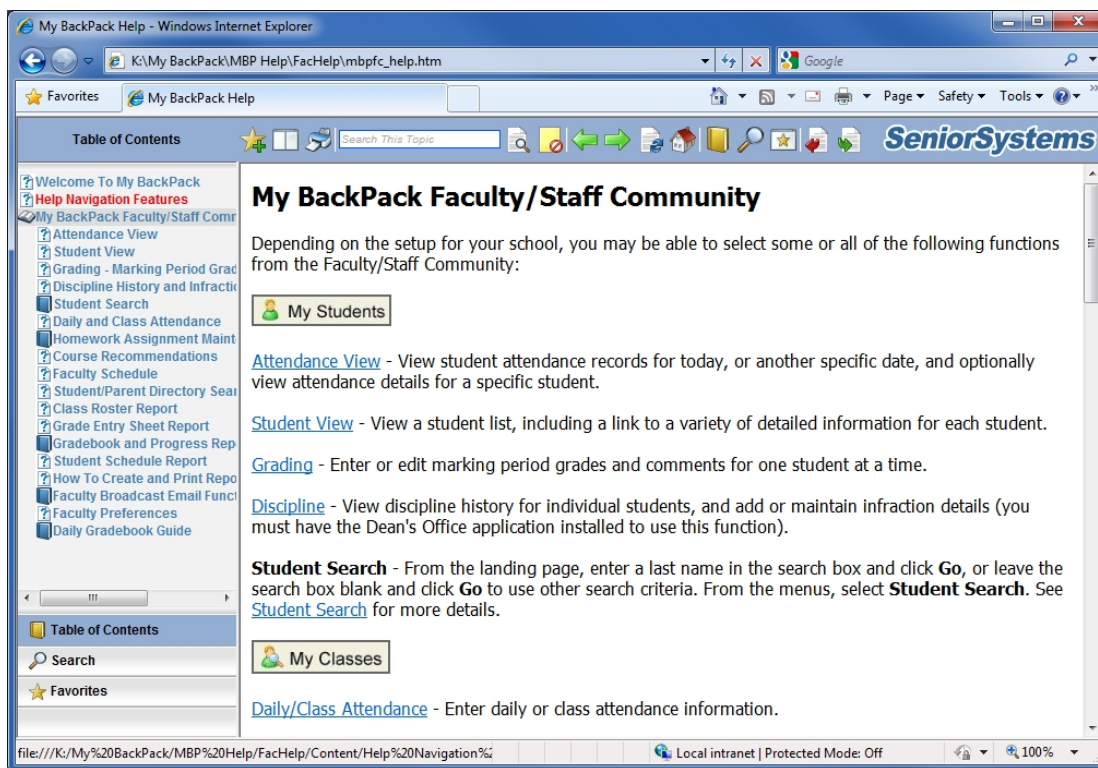
As always, please contact Senior Systems Product Support if you have any questions about these new and enhanced features!

Redesigned Help Facility For My BackPack

The Help interface for My BackPack has been redesigned and the administrative and faculty/staff sections now incorporate the material from several recently published My BackPack user guides, with topics cross-linked to make it easy to find related information.

Help for each My BackPack community is available by clicking the new Help icon in the community header on the landing page (far right side), or above the left side menu. In some cases, help is context-sensitive, providing information related to the currently selected function. There are a variety of new tools in the help window that enable users to search, navigate, save favorites, browse, and print help topics.

Next time you have a question relating to My BackPack functions, try the new help facility! For details about how to navigate and use some of the new help features, select **Help Navigation Features** in the Table of Contents on the left side of the screen.



New User Guides For My Backpack

We have recently published new user guides for My Backpack, including:

- Online Giving User Guide
- Online Statements User Guide
- My Backpack Administrator's Guide

These guides are in PDF format, and are available in your system Reference Guides folder, or from the Help menus in their related Senior Systems applications (Alumni/Development, Accounts Receivable, and System Administration, respectively).

The material from all of the My Backpack user guides is also incorporated into the new My Backpack help for the Faculty and Administrator Communities (see [Redesigned Help Facility For My Backpack](#) for more details).

Expanded User Name Field for My Backpack

The User Name field for My Backpack web users has been expanded from 20 characters to 50 characters. This will support the use of email addresses, or other types of expanded user names for My Backpack login purposes. Among other things, this can make it easier for parents, students, applicants, summer school/program registrants, and faculty who are not also database users to remember their My Backpack login information.

Authorize.Net™ Gateway Support for My BackPack

You can now use the Authorize.Net™ payment gateway with My BackPack payments. Setup via Merchant Card Administration and payment processing functionality is exactly the same as for the existing gateways, with the addition of a new button on the Merchant Accounts Setup screen and provision of the appropriate fields on the configuration screen for the account:

Merchant Accounts Setup

Merchant Accounts | Online Giving | Online Statement | Convenience Fee

Merchant Account List

Name	Provider	Action	Used by
Authorize.net Account	Authorize Net		Online Statement
NM DiamondMind Account	Network Merchants		Online Enrollment, Online Summer School Registration, Online Giving
Paypal Merchant Account	Paypal		Online Admissions

[Add Paypal Account](#) [Add Network Merchants Account](#) [Add Authorize Net Account](#)

Powered by Senior Systems, Inc.

Merchant Accounts Setup

Logged in as: Mrs. Lilly Abbott
Current School: Middle School

[Back to Merchant Accounts Setup](#)

Name:

Host Address:

API Login ID:

Transaction Key:

Transaction Cut Off Time: :

[Back to Merchant Accounts Setup](#)

[Apply](#) [Cancel](#) [Reset](#)

* - required field

Tracking Code Support For My BackPack

My BackPack now supports the use of tracking code (for services such as Google Analytics™) if your school participates in a website tracking service. There is a new field on the About My BackPack screen in the Admin Community of My BackPack where you can enter or update the tracking code provided by your service.

To enter or update tracking code for your website: select **About My BackPack** from the Administration menu in the Admin Community of My BackPack. Paste or edit the data in the Tracking Code field and click **UPDATE**.

About My BackPack

Logged in as: Mrs. Lilly Abbott
Current School: Middle School

Build Date and Time	: Friday, March 12, 2010 7:03 AM
Build Version	: 917
Database Version	: 917
Database Last Update	: Thursday, March 11, 2010 5:56 AM

Active Communities

Alumni/Advancement

Friends

Faculty/Staff - Teachers

Students

Administrators

Parents

SSL Certificate information is displayed here.

<script src="https://seal.verisign.com/getseal?host_name=%SERVER_NAME%&size=S&use_flash=YES&use_transparent=YES&lang=en"></script>

Tracking code is displayed here.

<script type="text/javascript">
var gaJsHost = (("https:" == document.location.protocol) ? "https://ssl." : "http://www.");
document.write(unescape("%3Cscript src='" + gaJsHost + "google-analytics.com/ga.js'
type='text/javascript'%3E%3C/script%3E"));
</script>
<script type="text/javascript">
try {
var pageTracker = _gat._getTracker("UA-12343014-1");
pageTracker._trackPageview();
} catch(err) {}</script>

Update

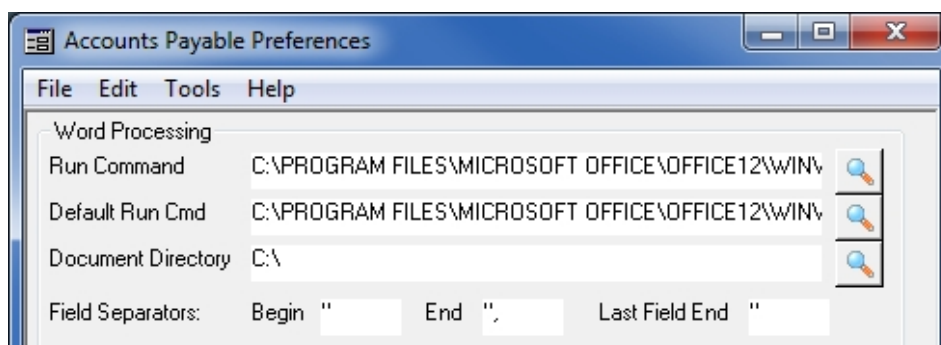
Copyright © 2002-2010 Senior Systems, Inc. All rights reserved. Warning: This computer program is protected by copyright law. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.
This product includes code licensed from RSA Security, Inc.. Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>. This product includes software developed by the Apache Software Foundation (<http://www.apache.org>). Contains spell checking software from Wintertree Software Inc. The Sentry Spell Checker Engine © 2000 Wintertree Software Inc.


Simplified Word Processing User Preferences

The Word Processing section of the User Preferences screen has been simplified to minimize the required input by users when configuring the word processing program to be used by mail merge functions. The only fields that are now required are the Run Command (directory path and program name of the word processor), the Document Directory (default for storing the resulting mail merge files), and the Field Separators (to be used between fields in the data file for mail merge).

In addition, if you are logged in as the schema owner, you can set a default Run Command value for new users. If all of your computers are configured in a similar fashion, this will make the preferences setup process for new users easier and less error-prone.

The User Preferences screen varies by Senior Systems application, but always includes the Word Processing section:



Each of the fields which requires the entry of a directory path now includes a  Search icon which can be used as an alternative to typing the entire path. Also, the Field Separators fields now default to the most common values to make setup quicker and easier for new users.



Web User Mailing For Applicants and Parents




There is now a third type of web user mailing that can be generated in System Administration specifically for applicants and parents. This functions in a similar way to the constituent and student/parent web user mailings in that it allows you to select (via several criteria and optional queries) the applicants/parents that you want to include. You can then generate postcards, labels, or envelopes, as well as a merge file that can be used to generate a customized form letter for each recipient.

For more details about the Web User Mailing function and the procedure, see the My BackPack Administrator's Guide that is available in your system Reference Guides folder.

Applicant/Parent Mailing Screens

Field	Usage/Remarks
Name Format	Use the Format dropdown to select the format for the Name. If you select 'As Saved', you can then use the Select dropdown to choose 'Full Name', 'Alternate Name' or 'Sort Key' to indicate the database field to use.
Include Preferred Name	Check this box to display an applicant's preferred name in parentheses.
Show Count	Check this box to display a count prior to printing or building the file, at which point you will have an option to cancel (otherwise, printing or building will begin immediately after you click Print or Build).
Exclude Blank Addresses	Check this box to indicate that records with blank addresses should not print or be included in the merge file.

Field	Usage/Remarks
Include Active Addresses Only	Check this box to indicate that addresses should only be included if they are marked as 'Active' in the database (otherwise all addresses that meet other criteria will be included).
Include Send Mail Only	Check this box to indicate that addresses should only be included if they are marked for 'Send Mail' in the database (otherwise all addresses that meet other criteria will be included).
Admissions Year	Select the Admissions Year that you want to use from the dropdown.
Status	You can select 'Inquiry', 'Applicant' or 'All', for the status type to include.
School Applying	You can select to include applicants to a specific school/division, or you can select 'All', 'None', or 'Some'. If you select 'Some', you can click the  Search icon to view a list and check the boxes for all those that you wish to include.
Form Type	For labels, postcards, or envelopes, select a standard form from the dropdown. This will also activate the Form Options button, which allows you to add a standard text line to be printed as the first line of the address, and (for envelopes) to print up to 2 additional lines of standard text in the lower left corner. This button also allows you to indicate your envelope feeding method, and to change printing options and printer setup information.
Start At Label Row/Column	For labels, you can enter a different starting row and/or column for printing if you are starting with a partial sheet of labels.
Save Only Mailing Data/All Data	For merge files, you can select to save only mailing data (names, addresses, etc.) or to save all available fields from the selected records (which can result in a significantly larger file).
Insert Field Names (Header)	For merge files, you can select whether or not to include a header row with the field names (this SHOULD be selected for use with Microsoft Word and other programs that use the field names for merge purposes).
Include Test Scores	Check this box if you want to include a test score, and then select the specific test score that you want to include. To change the selected test score, click the  Search icon to select a different one.
Include P2 Information	Check this box to include P2 information, where applicable.
Include Work Addresses	Check this box to include work addresses, where applicable.

Field	Usage/Remarks
Select Applicants	You can choose a query from the dropdown to select the applicants that you want to include. You can also view, create or edit queries by clicking the  Search icon.
Select Addresses	You can choose a query from the dropdown to select the types of addresses that you want to include. You can also view, create or edit address queries by clicking the  Search icon.
Sorting Conditions	If you want to use a particular sort order, you can select it from the Sorting Conditions dropdown. (You can also view, create, or edit sorting rules by clicking on the  Search icon.)
Mail History Description	You can optionally enter a description to be included on the Mailings tab for the inquiry/applicant in the Admissions application.
Sent Date	This date will be recorded in the Mail Sent Date for the user account when you click the UPDATE button.

Senior Systems PCI Compliance Policy and WISP Document

The following pages provide copies of documents related to Senior Systems' compliance with industry standards and regulations regarding security of cardholder data and the protection of personal information:

- The **Senior Systems PCI Compliance Policy** details the steps that Senior Systems takes to comply with Payment Card Industry Data Security Standards.
- The **Senior Systems Massachusetts Written Information Security Program** document indicates Senior Systems' compliance with Massachusetts state law regarding protection of personal data, and provides contact information for related questions.

Should you have any questions concerning these documents or policies, please contact Senior Systems.

SeniorSystems

March 29, 2010

RE: Senior Systems' PCI Compliance Policy

To Whom It May Concern:

The Payment Card Industry Data Security Standard (PCI DSS) is a set of twelve comprehensive requirements formulated by the major credit card companies to help enhance payment account data security. These requirements are organized into 6 basic principles that set the security standards for security management, policies, procedures, network architecture, software design and other critical protective measures. The object of the PCI Data Security Standard is to compel merchants to implement the necessary measures to protect cardholder information from hackers and con artists.

PCI Compliance is required for any company that stores, processes, or transmits cardholder data. Although Senior Systems does not store, process, or transmit cardholder data for its own business purposes, our Hosted Solution Software acts as a conduit for transmitting cardholder data when a client or client's constituent wants to pay online with a credit card. The data from the client/constituent passes through our My Backpack server and is forwarded on to a third party merchant and then back again. It is never stored or processed.

Despite this minimal contact with cardholder data and our status as a lower Level 4 Merchant, Senior Systems recognizes the importance of keeping any cardholder data secure and protected, regardless of whether that cardholder data is the school's or one of the school's constituents. As a company we have taken the necessary steps to be PCI Compliant and we will continue to be vigilant in protecting cardholder data that is entrusted to us.

Below you will find the twelve requirements grouped into six primary goals that were formulated by PCI Security Standard Counsel for PCI Compliance. Each requirement is followed by a brief explanation of the purpose of the requirement and what steps Senior Systems has taken to fulfill the requirement to be PCI Compliant.

BUILD AND MAINTAIN A SECURE NETWORK

REQUIREMENT 1: Install and maintain a firewall configuration to protect cardholder data.

Purpose: Firewalls are computer devices that control computer traffic between a company's network (internal) and untrustworthy networks (external), as well as traffic into and out of a company's internal trusted network. A proper firewall examines all of this traffic and blocks those transmissions that do not meet the specified security criteria.

Senior Systems Compliance: Senior Systems employs a dedicated server running Smoothwall®, a firewall software that examines all traffic to verify it meets the specified security criteria. The firewall and router configurations are set to deny all traffic except for authorized users and uses. The firewall software is regularly maintained and kept up to date. All configurations are reviewed at least once every six months

REQUIREMENT 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Purpose: Default settings are well known in hacker communities. By always changing these defaults when installing a system on the network, malicious individuals are prevented from using these default settings, account names, and passwords to compromise systems.

Senior Systems Compliance: Senior Systems invariably changes vendor-supplied defaults when installing any new software or hardware to the network system.

PROTECT CARDHOLDER DATA

REQUIREMENT 3: Protect stored cardholder data.

Purpose: If a company stores cardholder data it must use various technical methods to protect the data, such as encryption, truncation, masking, and hashing. By using these techniques it makes cardholder data unreadable to unauthorized users.

Senior Systems Compliance: Senior Systems does not store any complete cardholder data that would require PCI Compliance. The only partial cardholder data on the system are reference fields which only contain a card's last four digits and expiration date.

REQUIREMENT 4: Encrypt transmission of cardholder data across open, public network.

Purpose: Since the data is being sent over public networks it is more susceptible to being intercepted or diverted by malicious users. By encrypting the data it becomes unreadable to the malicious user.

Senior Systems Compliance: Senior Systems uses encryption/cryptography and SSL protocols for cardholder data sent over public networks.

MAINTAIN A VULNERABILITY PROGRAM

REQUIREMENT 5: Use and regularly update anti-virus software.

Purpose: There is a constant stream of new malicious software attacks against otherwise secure networks. A company must keep its anti-virus software up to date in order to repel the newest malicious attacks.

Senior Systems Compliance: Senior Systems updates its anti-virus software at least twice a day. In addition, the software and its responsiveness to attack are manually reviewed on a regular basis.

REQUIREMENT 6: Develop and maintain secure systems and applications.

Purpose: Over time, data thieves will discover vulnerabilities in systems and applications. A company must be vigilant in applying and developing security patches to any vulnerability.

Senior Systems Compliance: Senior Systems installs vendor-supplied patches immediately upon receipt of the patch. In addition, the system and applications are regularly monitored for vulnerabilities. For web applications, Senior Systems follows secure coding guidelines and uses a process to review custom application code for coding vulnerabilities.

IMPLEMENT STRONG ACCESS CONTROL MEASURES

REQUIREMENT 7: Restrict access to cardholder data by business need-to-know.

Purpose: Logic dictates that the more people who have access to cardholder data the greater the risk that this data will be used maliciously. Companies must employ “need-to-know” and “role-based access control” policies.

Senior Systems Compliance: As stated in requirement 3 above, Senior Systems does not store or process cardholder data. We merely transmit data between the client/constituent and a third party. This data passes through our My Backpack servers and is forwarded to third party merchants. Access to these servers is currently limited to three employees on a “need-to-know” basis. Periodic access is granted to another employee in special circumstances. That individual is given a temporary access ID and supervised until the task is completed. Thereafter the temporary ID is immediately erased from the system.

REQUIREMENT 8: Assign a unique ID to each person with computer access.

Purpose: By using unique IDs for each employee a company can maintain individual responsibility for actions and develop an effective audit trail per employee. This speeds up issue resolution and containment when misuse or malicious intent occurs.

Senior Systems Compliance: Each person who has access to the My Backpack servers that transmit cardholder data has a unique ID. Each ID is associated with that user’s password, which must be periodically changed.

REQUIREMENT 9: Restrict physical access to cardholder data.

Purpose: By restricting physical access, a company limits the number of individuals who can gain access to cardholder data or who might potentially introduce vulnerabilities into the network.

Senior Systems Compliance: As previously stated, the only contact Senior Systems has with cardholder data is the electronic transmission of this data through the servers in the Senior Systems Hosted Solution Center. Physical access to the Center is card and password restricted to four employees. Network access is restricted to the three individuals mentioned in Requirement 7 above.

REGULARLY MONITOR AND TEST NETWORKS

REQUIREMENT 10: Track and monitor all access to network resources and cardholder data.

Purpose: By having a system that links user access to the components they accessed, a company can generate audit logs and trace back suspicious activity to a specific user.

Senior Systems Compliance: Senior Systems has unique user IDs that can be traced back to a specific user. Any suspicious activity can be traced to a specific user. In addition, the Windows and Citrix consoles are manually reviewed daily to determine if there was any malicious access from the school's end-users.

REQUIREMENT 11: Regularly test security systems and processes.

Purpose: Companies have to continuously test and scan for new vulnerabilities to data systems that contain cardholder information. Testing must be frequent to combat this constant threat. Testing must include wired and wireless networks, network gear, servers, other system components, processes, and custom software.

Senior Systems Compliance: Senior Systems has a schedule for performing all the necessary testing to be PCI Compliant.

MAINTAIN AN INFORMATION SECURITY POLICY

REQUIREMENT 12: Maintain a policy that addresses information security.

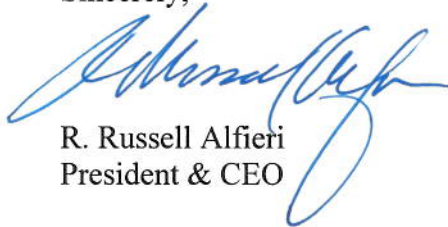
Purpose: By maintaining a clear policy a company can ensure it is PCI Compliant, that its employees are aware of the security standards and procedures, that it can help prevent vulnerability attacks, and that it can quickly address a malicious attack should it occur.

Senior Systems Compliance: Senior Systems maintains a clear comprehensive formal policy that ensures it is PCI Compliant. The policy identifies vulnerabilities and assesses risk on at least an annual basis; provides daily procedures for Compliance; assigns responsibilities; teaches security awareness; lists employee and third-party screening practices; and provides a plan for immediate response to a breach.

The PCI Security Standard Counsel has divided merchants into 4 levels with validation criteria for each level. Senior Systems follows the validation requirements for a Level 4 Merchant. This includes submitting an annual Self-Assessment Questionnaire and having a quarterly scan of the cardholder data network.

PCI Compliance is not a onetime thing. It is a continuous process that requires dedication, commitment, and vigilance by a company to secure and protect cardholder data. Senior Systems will continue to follow the 12 requirements stated above and will take any other necessary steps to ensure PCI Compliance.

Sincerely,

A handwritten signature in blue ink, appearing to read 'R. Russell Alfieri', is written over the printed name and title.

R. Russell Alfieri
President & CEO

SeniorSystems

March 1, 2010

RE: Massachusetts Written Information Security Program (WISP)

To Whom It May Concern:

Senior Systems respects and appreciates the absolute need for proper security and safeguarding of personal information contained in both paper and electronic records. We are in support of and fully compliant with Massachusetts' Standards for The Protection of Personal Information [201 CMR 17.00], the latest in state regulations taking effect on March 1, 2010.

If you have any further questions, please contact:

Brian Dombrowski, Technology Manager

briand@senior-systems.com

(888) 480-0102, ext. 271

Steven P. Kearney, Of Counsel

stevek@senior-systems.com

(888) 480-0102, ext. 251

R. Russell Alfieri, President & CEO

russa@senior-systems.com

(888) 480-0102, ext. 211

Sincerely,

R. Russell Alfieri
President & CEO