



Employer Information Technology Guide



Contents

1.	Introduction	2
2.	Background	2
3.	System specifications.....	3
4.	Security	4
5.	Mobile access	5
6.	Configuring your network	5
7.	Preparing user data file for import	6
8.	Frequently Asked Questions	6
	Is our employee’s information secure?	6
	What type of employee information is retained?	7
	Who can access Charities At Work Powered by Andar/360 ?	7
4.	How are credit card transactions handled?	7
5.	Contact for additional questions?	7
	Appendix A - Third Party Service Providers	7
	1) iWeb – iWeb Technologies	Erreur ! Signet non défini.
	2) CyberSource	Erreur ! Signet non défini.

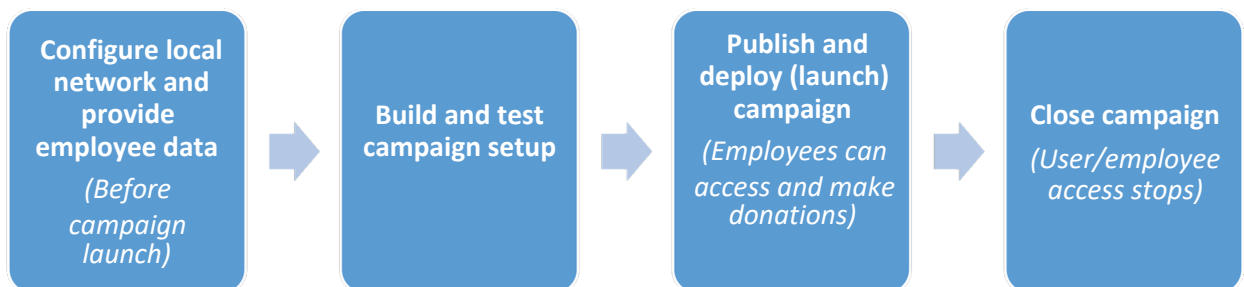
1. Introduction

Thank you for considering (or choosing) to use the **Charities at Work** tool for your campaign. Your department has an additional role to play in ensuring that employee donations made through the **Charities at Work** tool can be processed easily and effectively. This guide is meant to provide some technical information regarding the application as well as some IT tasks needed to ensure a smooth campaign.

2. Background

Charities at Work is a completely web-based platform that allows your organization to deploy and manage a customized giving campaign to your employees. The platform allows employees to pledge amounts to HealthPartners (or its member charities), or to any nationally registered charity in Canada of their choosing. Employee pledges can be made with a credit card in real-time (e-commerce) or they can opt to donate via payroll deduction.

The overall process is as follows:



3. System specifications

Efforts have been made to ensure that the **Charities at Work** solution is secure and safe. The solution is hosted in Tier 3 data centers, and the infrastructure is managed by Andar Software’s skilled engineers and partners. **Charities at Work** is a Java/JSP (JavaServer Pages) based application built on a Tomcat web server using the latest and most secure Java application libraries.

A summary of some of the key technical specifications are provided below.

Description	Details
Virtual Servers	Windows Server 2019 64-bit hardened virtual servers, with VMware vSphere Virtual Machine Encryption, running Next-Gen AV w/ EDR agent, IDS/IPS w/ XDR agent, Vulnerability Management agent, and Remote Monitoring & Management agent. Located in Tier 3 data centers in Ottawa, Ontario with redundant firewall appliances, and cloud-based Web Application Firewall solutions. Java 13 on Tomcat 9, SQL Server 2019, Javascript, jQuery 3.6, jQuery-UI 1.13.2, Bootstrap 4.3. <i>(at the time of this writing)</i>
Application language(s)	Server 2019, Javascript, jQuery 3.6, jQuery-UI 1.13.2, Bootstrap 4.3. <i>(at the time of this writing)</i>
User connection security	HTTPS/TLS All connections are encrypted, logged, and monitored 24/7/365.
Credit card transactions	Transaction management through CyberSource. Application settings offer the use of a “hosted” Cybersource credit card entry page that bypasses all internal servers and therefore places Andar/360 in the best PCI Compliance Level.
Application framework	Java/JSP (JavaServer Pages) based application built on a Tomcat web server using the latest and most secure Java application libraries.
Third-party service providers (Refer to Appendix A)	CyberSource - e-commerce
Backup/Continuity	Virtual machines (VMs) are backed up twice daily, stored locally and replicated to secure S3 Bucket with 1-7 years retention. Files and Databases are backed up 4 times daily, stored locally and replicated to secure S3 Bucket with 1-7 years retention. VMs are replicated continuously to Disaster Recovery site in Airdrie, Alberta.

4. Security

Completely hosted in Tier 3 data centers managed and secured by Andar Software and its partners. **Charities at Work** does not install any software on the user's computer.

Browsers and operating systems:

- **Charities at Work** is compatible with all major A-Grade browsers (Chrome, Edge, Firefox, and Safari), but will not be accessible with a browser release being not anymore supported (like Internet Explorer)
- Works with any operating system (Windows, Mac OS, etc...) as long as the browser is compatible and supported

Users:

- All users are provided with unique user id and password
- User account creation requires authorization from primary contact at HealthPartners.
- Users are in control of personal information through their profile page
- Users can have different levels of access and rights to system activities based on their pre-defined role in the campaign

Security compliance certifications:

Andar Software's Hosting environments achieves the following certifications:

- Canadian Federal Government Security Protected B
- Canadian Federal Government Controlled Goods Certified
- CSAE 3416 Type II, CSAE 5025, ISAE 3402, ISAE 3000
- GLBA and PCI DSS
- PCI Compliancy
- PIPEDA, PHIPA Compliancy
- SOC 1, 2 and 3
- UTI Tier III Certified

Credit card AOC: not required for **Charities at Work** because no credit card information is seen, captured, or handled by **Charities At Work**. Required certifications are held by CyberSource.

Credit card transactions:

These transactions are managed through CyberSource:

- Certified PCI application, adhering to Data Security Standards (PCI DSS), level 1 compliant
- Certified SSAE 16 SOC 1 Type 2, CSAE 3416 and ISAE 3402
- Certified OWASP ASVS V2, Level 1

- Certified hardened against Metasploit Framework (v4.16.9) WMAP Web Scanner (v1.5.1) exploits

Emails sent by *Charities At Work*:

Emails from Andar/360 uses encrypted virtual SMTP servers with the following:

- SMTP servers located in Tier 3 data centers in Ottawa, ON & Airdrie AB.
- All connections use encrypted port 587 and secure protocols (SSL / TLS)
- Emails never retained on servers for more than 24 hours.
- SMTP servers relay through Email Security Gateways to provide additional security protection against misuse, spamming and malware.
- SMTP servers with built-in capabilities to validate recipients and provide real-time analytics, alerting, and reporting.
- Public IP Addresses of SMTP servers added to customer's 'Sender Policy Framework (SPF)' record.
- Customers encouraged to configure DKIM & DMARC within the domain names used as the Sender of Andar/360 emails.
- SMTP Logs are retained for 7 years.

5. Mobile access

Charities at Work was designed with mobile access in mind, without the use of a stand-alone mobile app. As long as the device's browser supports A-Grade browsers there should be no issue using the application on a mobile device.

6. Configuring your network

To ensure that your employees have a good user experience using *Charities At Work*, we ask that you ensure that the following elements are in place prior to the campaign launch date.

- **Configure firewall** – to allow access to the *Charities at Work* sites:
 - o Allow access to <https://portal.healthpartners.ca/>.
- **Configure spam filters** – to allow emails from *Charities at Work* tool:
 - o Whitelist emails from domains:

- 📧 @healthpartners.ca
- 📧 @partenairesante.ca
- 📧 @partenairesante.quebec

o In addition, the following IP addresses should be whitelisted for Andar Software

- | Hosting's SMTP servers:
 - ☒ 199.246.24.125/32
 - ☒ 199.246.24.128/32
 - ☒ 199.246.24.164/32

- **Cookies** – Some cookies are stored to the user's computer. This is done to track certain user data, as well as to prevent Cross-Site Request Forgery (CSRF)
 - o Browsers should be configured to allow cookies and/or browser security settings should establish **<https://portal.healthpartners.ca/>** as a trusted site.

7. Preparing user data file for import(if applicable)

In order to create user accounts in the **Charities at Work** application we will need to upload your organization's employee information. The upload is done via an Excel file that you or someone in your payroll or human resources department will need to populate.

Once the data file is ready, please send it to your campaign manager for review and approval so that it can be sent to us for upload into the system.

A sample of the file is provided in Appendix B.

For detailed instructions, see the document:

"CharitiesAtWork_Employee_List_Template_instructions.pdf"

8. Frequently Asked Questions

1. Is our employee's information secure?

Your employee's information is securely stored on encrypted virtual servers located in Canada.

Within the Andar/360 application, there are many security options in place to add additional layers of security to your data. These include, but are not limited to:

- reCAPTCHA v3 (Google) during gift entry
- Automated "Security Event" Notifications to administrators
- Customizable User ID and Password Protection
- Optional Credit Card Verification Settings (Address Verification, CVV)
- Multi-Factor Authentication (MFA)

2. What type of employee information is retained?

The following information is retained in HealthPartners databases:

- The employee information as provided in the upload(if applicable)
- Employee's donation details such as amounts and to what charitable organization
- The Employee's preferences related to sharing their contact information with HealthPartners or other charities.
- The name and address of the credit card holder are retained to produce the tax receipt for the donor.

No credit card information is entered into the database. All credit card processing data, including name and address of the credit card holder, credit card number, expiry date and security code (CVV) are managed exclusively by CyberSource to maintain PCI compliance.

3. Who can access *Andar/360* ?

Only employees who have been uploaded into the system will have access after they accept the email invitation from HealthPartners to complete their account creation by clicking on the link provided in the email. Other employees can be invited to create an account if added by someone with the appropriate security role/rights. Andar Software | Hosting staff for the sole purpose of providing support.

4. How are credit card transactions handled?

All credit card transaction payments are processed by CyberSource, a certified service provider (see Appendix A), through their secure PCI-compliant e-commerce gateway. No credit card information is seen, captured or handled by HealthPartners or any other party.

5. Contact for additional questions?

If you have any other questions do not hesitate to contact Lisa Poulin at 613-562-1469 or 1-877-615-5792 ext.: 225 or email us at info@healthpartners.ca

Appendix A - Third Party Service Providers

1) Andar Software LTD

Mississauga, Ontario

www.andarsoftwware.com

- Cloud Hosting services provided in Tier 3 Canadian based data centers.

2) CyberSource

www.Cybersource.com