Call2Recycle

GreenTrax
Web Portal
Security Application

v.1.0_20150615

DRAFT

Revision History

VERSION	DATE	NAME	DESCRIPTION
Original 1.0	5/26/2015	Joe Walker	Original
Revision 1.1	6/15/2015	Joe Walker	First draft posted

Table of Contents

Statement of Intent

This document delineates our intended policies and procedures for end-user (i.e. customer) data security and technology access for the GreenTrax web portal and supplementary systems. This document will also cover the chain of custody of the data for enterprise use, and the procedures for repurposing this date for other internal/external applications.

The following terms and acronyms will be used throughout the document in a controlled manner by the definitions below:

- **End-user**: anyone who is using the intended computing application, such as a web portal
- **GreenTrax security application**: the combined systems, policies, and processes used to assure end-to-end security of the data generated from the GreenTrax application
- **IT**: Information Technology, systems and personnel
- **Web portal**: a web browser accessible user interface for a consolidated systems infrastructure. Usually a website interface augmented by application stacks beyond the regular HTML scheme.

An important aspect of the GreenTrax web portal is to facilitate customer access to enterprise processes and allow a suitable level of automation and self-service within the system to leverage increased efficiency. With access comes concerns about security and enforcement of strict process controls. This document summarizes our recommended procedures to assure that these security concerns are addressed and achieved in every real application of the system. The GreenTrax security application is as much a coordinating concept and focus as it is real procedures and software applications in place to provide the security for the system as a whole.

Modifications to this document may be made to ensure the continued security of the system and protection of end-user data.

Objectives

The principal objective of the GreenTrax security application is to develop, test, and document a well-structured and easily understood coterie of processes and sub-applications that will assure the management and access of GreenTrax generated data throughout the several coordinating layers of the user interface, background IT systems, as well as the chain of custody of the data when used by other segments of the enterprise. The security application includes the following focal aspects:

- The IT systems and physical computing infrastructures that the web portal uses for process execution are secure and controlled by authorized IT personnel. This is referenced within the security application as End-user Layer One Security (L1Sec).

- The end-user interface, access means, and coding vectors that the web portal uses for process execution are deployed and used as intended—that public exposure is controlled by authorized IT personnel and project managers. This is referenced within the security application as End-user Layer Two Security (L2Sec).
- The use of end-user data follows a chain of custody throughout the enterprise and is controlled by authorized project managers. This is referenced within the security application as End-user Layer Three Security (L3Sec).

1 Systems Services and Physical Computing Infrastructure – End-user Layer One Security (L1Sec)

1.1 Overview

It is necessary for the systems infrastructure that constitutes the physical and computing basis of all the web portal processes to be properly structured and controlled. This infrastructure includes internal, enterprise IT resources and databases, enterprise software, network security processes, third-party hosted services within third-party controlled physical property and servers—as well as any other IT systems were needed. L1Sec is mostly concern with the internal IT systems infrastructure of the corporate and hosted end-points of all GreenTrax web portal processes and data storage locations traversing the web portal.

Whenever changes are made to the infrastructure, they are to be fully tested with the security application and appropriate amendments should be made to the documentation. This will involve the use of formalized change control procedures under the control of the IT Director.

1.2 Call2Recycle IT Systems Infrastructure Security

As all the internal data for the GreenTrax web portal is retrieved from and stored within Call2Recycle's own internal enterprise application, Sage SalesLogix, the first layer of any security application must very well start and end with the native security features of the company's own IT processes and controls.

The Call2Recycle IT Systems Infrastructure is under the control of the IT Director.

1.2.1 Call2Recycle Network Security

The first line of defense in any local network is established at the network firewall, and how that IT infrastructure is implemented and administered. The firewall infrastructure in many cases becomes the *de facto* demarcation between the external, and unsecured, publicly accessible Internet and the secured local area network (LAN) that all your enterprise services resides and communicates over. As network data flows between the computers within a LAN and the Internet, all the data is passed through and scanned by the enterprise firewalls. Any network traffic that does not first flow through the enterprise firewall infrastructure is by definition a breach of network security.

Depending on the firewall manufacture, each has a host of native scanners that are used to filter network data. These scanners are combined with security policies setup by the IT administrators that strictly control computer and user access to the data from the firewall—implicit permissions that tell the firewall who can send what data where, using what services and computers. Without such an implicit permission established within the firewall, it will by default block access between LAN and Internet communications, and if the firewall infrastructure is designed to, can even block network access between segments of the LAN as well. In essence, the basic state of any firewall is to stop network traffic in all cases unless told otherwise.

Call2Recycle uses a combined firewall infrastructure of FortiNet and TippingPoint manufactured security appliances controlling the access of SalesLogix and establishing the egress of SData feeds to the hosted web server at the third-party location. Due to the setup of the network security, end-users within the corporate network have direct, secure access to SalesLogix via their login credentials. End-users coming from the Internet have no direct access to SalesLogix at all, accept through two highly secure gateways: VPN access and SData.

VPN access is secured through implicit setup of the user by IT administrators and use of assigned login credentials and/or certificates. VPN access allows an end-user access to LAN resources as if they were inside the corporate network. This access is secured by encrypting all point-to-point network traffic between that end-user and the enterprise firewall infrastructure.

SData feeds security is covered in the following sections below.

1.2.2 Call2Recycle Facility Security

The physical servers and storage appliances where the SalesLogix processes and data resides is located entirely within the Call2Recycle Atlanta office. Physical access to our Atlanta office is secured through controlled building access and internal suite access via a RF badge access card assigned to individual users. Once inside the suite, the person would have to have further card permissions assigned in order to access the server room.

The following are the three security categories for physical access to the Atlanta office facilities:

- Physical access to the building is limited to associates of tenants within the building—permission is assigned by building management
- Physical access to the Call2Recycle suite is limited to employees of the company and designated visitors—employee permissions are assigned by IT personnel and visitor access by employee authorization and supervision
- Physical access of the server room is limited to IT personnel only—permission is assigned by IT personnel

1.3 Third-party Hosted Web Servers and Physical Facilities

Call2Recycle uses a third-party leased web server hosted by RackSpace US, Inc. Like any IT systems solution, there are always pros and cons when it comes to a specific choice to implement, and hosted services are no different in this respect.

The IT department's determination of using a hosted solution was made after a consideration of the following attributes:

- The down-side of a hosted service is that corporate IT does not have direct access to the server, the network it uses, or any of the physical infrastructure that constitutes its computing resources. With a hosted service, we the customer are depended wholly on the host provider's own security applications and our ability to leverage it within the setup of their service for our needs.
- The positives of a hosted service is that it remains outside of the enterprise firewall, so we do not have to potentially compromise LAN security allowing external access to any internal services for potential customers. Most internal security applications are depended upon a point-to-point control of the environment in order to be deployed accurately, which is never the case with random customers. If the hosted web server were to become compromised, it does not have the necessary LAN access to compromise the internal network of the enterprise.

Call2Recycle's use of Third-party IT Systems Infrastructure is under the control of the IT Director.

1.3.1 Hosted Web Server and Administration

The hosted web server we use as the computing platform for the end-user interface portion of the GreenTrax web portal has the following configuration:

- Linux OS – HP DL385 G2 Linux
    - Antivirus: Sophos
    - Public IP: 98.129.187.243/30

    - Internal IP: 10.244.64.47
    - Rackspace support and monitoring
- Firewall management – Cisco ASA device
- Internal Rackspace security application
- Remote server access hardening

1.3.2 Rackspace Hosted Services

Rackspace, along with most third-party hosted services, implement the following IT systems infrastructure:

- Secured datacenters where the server hardware and storage and physically located
- Hardened network infrastructures—LAN and site-to-site networks
- Virtualization of server operating systems
- Multi-tenancy of the virtualized environment
- Account security applications and customer administration

As per their published corporate documentation into the internal infrastructure of their service, they implement the following described operational security applications and processes. Rackspace Hosting's policies and procedures set a high standard that each employee, consultant, and third-party service provider is required to follow.

These corporate standards cover key functions like:

- Password based access
- Password expiration
- Automatic workstation locking
- Documented change management and escalation procedures
- Onboarding training
- VPN-base access
- Access that are monitored and independently audited

Rackspace maintains documented operational procedures for both infrastructure operations and customer-facing support functions. Newly provisioned infrastructure undergoes appropriate testing procedures to limit exposure to any hardware failure. Documented procedures and configuration version controls provide protection from errors during configuration of enterprise deployments. Changes to an existing infrastructure are controlled by a technical change management policy, which enforces best practice change management controls including impact/risk assessment, customer sign off, and back-out planning.

Rackspace Hosting participates in and maintains the following audit reports, certifications, and documentation:

- SSAE 16 / ISAE 3402 (formerly SAS70 Type II) Audit Reports
- Safe Harbor Self-Certification

- ISO 27001 Certification(s)
- PCI Attestation of Compliance & PCI DSS Validated Service Provider
- CDSA Certification
- SOC2 Data Centers in Security & Availability Report
- SOC3 Data Centers in Security & Availability Report

Internally, OpenStack internal communications are performed as RESTful API calls that can be secured via SSL/TLS certifications. Looking forward, OpenStack's security groups are actively advancing Firewall-as-a-Service and other OpenStack networking features enabling multiple levels of software defined network isolation.

A core element of OpenStack is its support for multi-tenancy. Rackspace implements this by initially installing a virtual computing environment configuration that ensures isolation between tenants within the datacenter shared resources. Tenant isolation is used to prevent unrestricted communication between business units or application domains. This best practice safeguards against cross-VLAN communication by restricting ingress traffic based on destination port and source IPs. If requested, configurations are also possible that could allow inter-VLAN communications. The OpenStack Image Service based on the Glance project, as implemented in the Rackspace Private Cloud, can be integrated into an Enterprise's existing change management and image release process. This allows the use of an organization’s existing, hardened images developed by their own IT departments.

Within the Rackspace service, accounts can be authenticated using either internal or external authentication protocols, such as LDAP and Active Directory. This allows enterprises to reuse their existing infrastructure and security applications on account management procedures. Account roles provide fine-grained authorization over specific actions and are assigned to designated users by the administrators of the customer account. Customers can also define custom roles to meet specific compliance or operational needs (e.g. segregation of duties).

Whether the service is hosted at a Rackspace datacenter or at a customer's datacenter, the Rackspace support team will adhere to both Rackspace's corporate as well as the customer's policies and procedures.

More information about Rackspace services can be found at the following location:
http://support.rackspace.com/

The Rackspace Privacy Policy can be found at the following location:
http://www.rackspace.com/information/legal/privacystatement

1.4 Sage SalesLogix Native Security

SData is a web enabled API for SalesLogix allowing point-to-point interaction with SalesLogix databases from an external application or website. SData is designed as a specification that is implemented via RESTful web services, which means service providers are not limited to using SData with a particular technology such as exclusively via .NET. SData works by sending and receiving XML payloads via a URL over network infrastructure.

By itself, SData is not secure—it relies on the native security features in place of a well-developed IT networking infrastructure and public-facing interface. Like most network protocols, it is clear text, and if the network packets are intercepted, the content of the SData exchange can be potentially obtained by an unauthorized third-party. This critical process constitutes an obvious and significant vector of attack for data security breaches in any IT infrastructure that is not properly implemented.

Call2Recycle's deployment and use of the Sage SalesLogix enterprise application is under the control of the IT Director.

1.4.1 Sage SalesLogix SData HTTPS Security

In a properly deployed network and systems infrastructure, SData is secured by implementing HTTPS functionality between the SalesLogix servers inside the secured Atlanta LAN and the web server executing the GreenTrax process request currently on the secure Rackspace hosted LAN. HTTPS consist of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and to protect the privacy and integrity of the exchanged data, usually be means of asymmetric encryption based on a shared security certificate. Through this process, HTTPS creates a secure tunnel for the SData communication link between the two secured LANs over the unsecured Internet.

This shared security certificate is stored on both the Atlanta LAN firewall and the Call2Recycle web server that is hosting the GreenTrax web portal. The security certificate shared between the GreenTrax web server and the end-user web browser will define and set the level of encryption used to secure the HTTPS communications.

1.4.2 Sage SalesLogix Servers Security

The SalesLogix servers are secured behind the Atlanta LAN network and are strictly controlled through the physical barriers of the facility security and the login securities of the enterprise user accounts.

Please see the section on Call2Recycle IT Systems Infrastructure Security for more information on this part of the security application.

1.4.3 Oracle Database Security

The Sage SalesLogix databases reside within Oracle Database 10g instances. When SData makes a call back to the SalesLogix servers, the SalesLogix servers in turn make an internal call to their databases provisioned within the Oracle application. If a vector of attack could compromise the Oracle database, then this third-party would gain feasible access to all the data within the GreenTrax system, effectively circumventing the many other strata of security implemented at the higher layers of the system stack. Due to this practicality, it is important that the security of the Oracle database be considered with the GreenTrax security application.

Much like the SData protocol, Oracle databases by themselves are not inherently secure—they rely extensively on the native security features in place of a well-developed IT systems infrastructure. Although, given that they require no public-facing interfaces—for applications leveraging SData handle this part of the process—these databases are relatively easy to secure behind solid LAN firewalls and internal access procedures.

Please see the section on Call2Recycle IT Systems Infrastructure Security for more information on this part of the security application.

2 Web Portal and Code Vectors of Access – End-user Layer Two Infrastructure (L2Sec)

2.1 Overview

The highest profile component of the entire GreenTrax system is the end-user browser-based web portal. This interface itself requires a close coordination of multiple IT systems, coded application developments, and behind the scenes access to internal enterprise IT resources. L2Sec is mostly concern with design of the web portal interface, vectors of end-user access to the interface, and hand off of submitted end-user data through the interface to internal IT systems infrastructures within the L1Sec level.

Whenever changes are made to the web portal deployment and code vectors, they are to be fully tested with the security application and appropriate amendments should be made to the documentation. This will involve the use of formalized change control procedures under the control of the IT Director with assistance from the GreenTrax project manager.

2.2 Web Portal Access Security Features and Data Security on the End-User's Device

The GreenTrax web portal relies on several coordinated systems offering a multilayer application of security covering all processes of the web server, end-user, and third-party access vectors. Implementing secured HTTPS communications and strict control over the DNS and public IP addresses used to access GreenTrax become the main features of this security application at this stage of the GreenTrax system. End-user security is implemented by the end-users themselves, and all Call2Recycle can do is recommend each leverage the best practices in managing the security features of their own devices. Each are discussed below.

The GreenTrax Web Portal access security is under the control of the IT Director.

Data security on the end-user's device accessing the GreenTrax web portal via their assigned user account is under the control of the end-user.

2.2.1 GreenTrax Access via HTTPS

The GreenTrax web portal is accesses by the general public using the standard Hypertext Transfer Protocol (HTTP). This protocol is the communications foundation for all web sites accessed through a variety of computing devices. By itself, HTTP is not secure—it relies on the native security features in place of a well-developed IT networking

infrastructure and public-facing interface. Like most network protocols, it is open-text, and if the network packets are intercepted, the content of the user to web site exchange can be potentially obtained by an unauthorized third-party. This critical process constitutes an obvious and significant vector of attack for data security breaches for an IT infrastructure that is not properly implemented.

In a properly deployed network and systems infrastructure, the user to web site interface is secured by implementing HTTPS functionality between the web servers inside the secured Rackspace LAN hosting the GreenTrax web portal and the end-user's computing device, whether it is their desktop, laptop, mobile device, etc. HTTPS consist of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and to protect the privacy and integrity of the exchanged data, usually be means of asymmetric encryption based on a shared security certificate. Through this process, HTTPS creates a secure tunnel for the web browser communication link between the server and client over the unsecured Internet. This shared security certificate is stored on both the Call2Recycle web server that is hosting the GreenTrax web portal and, once accepted, by the web browser of the end-user's device.

The security certificate shared between the GreenTrax web server and the end-user web browser will define and set the level of encryption used to secure the HTTPS communications.

2.2.2 Control of the GreenTrax DNS and IP Addresses

The second feature of the web portal access security is the strict control over the DNS and IP addresses authorized for GreenTrax web portal access. This control is exercised by the Call2Recycle IT department, and assures that all points of public access to the GreenTrax systems are provided by servers deployed and monitored in accordance with the GreenTrax security application.

2.2.3 Process Flow within the GreenTrax Service

The flow of processes within the GreenTrax service offers more opportunities for the security application to be employed. These processes handle data movement between the web portal's end-user access (i.e. account logon) and the back-end SData communication link between the web server and the SalesLogix servers and databases. These computation processes are handled predominately on the web server that the end-user is accessing the web portal on, and partly within the web browser of the end-user's device. These processes leverage the security application as follows:

- SData requires username/password authentication during each request for data
- GreenTrax web portal requires additional username/password authentication in order to access the application layer of the GreenTrax system, namely queries of the SalesLogix databases
- Important GreenTrax session data, including access authentication, is killed after the web browser is closed unless the client's browser is set to override this

With these steps in place, the security application's focus is to assure that no information from SalesLogix is being stored by our processes outside of our secured Atlanta LAN network, and that the data is secured and the end-user is authenticated upon each request.

2.2.4 Disclaimer for Security on the End-User Device

Call2Recycle can guarantee the security of the web server and offer the security certificate for HTTPS for secure communications between us and the end-user's web browser, but we cannot guarantee the security environment on the end-user's computing device. This can only be guaranteed by the end-user themselves. Once the web portal data is on their device, they accept responsibility for its security.

Compromising the end-user device is a standard vector of attack by third-parties to access user data. Once the device is compromised, perhaps by a key-logger installed on the device, and if the attacker can discover the user's password, then the attacker can mimic the end-user on the web portal and access all the content and functions that are assigned to them. It is the responsibility of the end-user to notify Call2Recycle in case of a suspected security breach of their GreenTrax account via their device. Fortunately, the attacker would not be able to access other user accounts not associated with this end-user.

2.3 Security Features for the GreenTrax Logon Accounts

Assuring the security of GreenTrax web portal logon accounts is an important element in the GreenTrax security application as a whole. Compromising accounts by third-parties wanting to gain unauthorized access to the system has become a popular and efficient vector of attack against segments of web portal-based systems with public facing interfaces. The following processes below are designed to harden the system in order to protect against some of the know vectors, but allows enough system flexibility to adapt to unknown vectors.

Security features for the GreenTrax logon accounts are under the control of the IT Director.

2.3.1 Security Process for the New Account Access Setup

Account request and setup by the end-user is a possible vector of attack by third-parties within the GreenTrax system. In order to mitigate this threat, we have implemented the following process:

- When a new contact is set up in SalesLogix we include both a temporary password (in real text) entry along with a flag to indicate when they have logged into GreenTrax web portal for the first time. New records have this flag set to 0/false, indicating that they have not ever logged onto the portal.
- This flag is used in conjunction with the real text temporary password to check the validity of the account and force them to reset their password (see below) to a permanent and secure password known only to the contact. The password is stored in SalesLogix only in a hashed formed.
- Once the first time login flag has been set to 1/true, we will follow the 'Forgot Password/Reset Password' process for existing contacts.

2.3.2 Security Process for the Account First Time Access Process

As a follow up the new account setup process, first time login offers its own unique vectors of attack. In order to mitigate against this threat, we have implemented the following process:

- When a new account logs in for the first time and provides their temporary password, the GreenTrax system checks for their first time login flag (see above). If this is a first time login, the contact will be directed to the 'Forgot Password/Reset Password' process in order to set a permanent password for their account. This password is then stored in SalesLogix only in a hashed formed, overwriting the temporary password.
- Until this reset password process is completed, and the first time login flag set to 1/true within SalesLogix, the account will be unable to access any other areas of the web portal.
- After the permanent password is set, the browser session will continue normally and they will have access to any their authorized areas within GreenTrax.

2.3.3 Forgot Password/Reset Password Process

In parallel to the two processes above, both leverage the 'Forgot Password/Reset Password' security function. At any time, an existing account can request a password reset by providing the email address for their contact record. A single-use link/URL will

then be provided to them via the email address on-file along with instructions for completing the reset process for their account's password. Using only the on-file email address is a security feature to authenticate the end-user requesting the password reset—they would also have to have access to this email address in order to receive the link/URL.

The requesting end-user then clicks on this link in the email and provides the new permanent password via a simple form on the GreenTrax web portal. A required confirmation is added to ensure that they have provided a password they intent to use for the account along with security recommendations for strong password selection. Once the password is reset they will be able to log in and access the GreenTrax web portal per their authorized access within the system.

3 Information Applications and Chain of Custody – End-user Layer Three Infrastructure (L3Sec)

3.1 Overview

When any security application handles continuous streams of dynamic data, the system and its processes must remain somewhat malleable and adaptive to the variables of the enterprise's use of the data in order to maintain its viability and efficiency. Unlike L1Sec and L2Sec that resides on mostly physical infrastructure and IT processes—once put into place rarely change without engineered restructuring usually through a formal planning procedure—L3Sec has to remain more organic in nature. Its security principles must be robust enough to grow as new applications (i.e. an agreed upon use of the end-user's data as opposed to IT software) of the data are determined and old applications are discontinued. L3Sec is mostly concern with the chain of custody of data and compliance to industry best practices as the applications for end-user data are determined and redefined throughout the enterprise.

Whenever changes are made to the application goals and usage of data, they are to be fully tested with the security application and appropriate amendments should be made to the documentation. This will involve the use of formalized change control procedures under the control of the GreenTrax project manager with assistance from the IT Director.

3.2 Call2Recycle Privacy Policy

The Call2Recycle Privacy Policy applies to all information collected or submitted on the Call2Recycle websites. On some pages, customers can order products, make requests, and register to receive materials, and in order to better protect their privacy we provide this notice explaining our online information practices and the choices made by the enterprise about the way information is collected and used. To make this notice easy to find, we make it available on our homepage and at every point where personally identifiable information may be requested.

Some of the types of personal information collected at these pages are:

- Name
- Address
- Email address
- Phone number
- Language Preference
- Country

For more information on the Call2Recycle Privacy Policy:

http://www.call2recycle.org/call2recycle-privacy-policy/

The Call2Recycle Privacy Policy is under the control of its authorized project manager.

3.3 PCI Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card, to including: Visa, MasterCard, American Express, Discover, and JCB.

The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire for companies handling smaller volumes.

For more information on the PCI DSS and compliance:
http://pcidsscompliance.net/

The Call2Recycle PCI Compliance process and enforcement is under the control of its authorized project manager.

3.4 Process Resources and Data Classification

The Call2Recycle Process Resources and Data Classification process and enforcement is under the control of its authorized project manager.

3.4.1 End-user Data Objects

3.4.1.1 Account Information

3.4.2 Data Classification Tagging and Handling Processes

3.4.2.1 Confidential

3.4.2.2 Internal Use Only

3.4.2.3 Public

3.5 Specific Security Procedures (not otherwise listed)

These additional Call2Recycle Security Procedures are under the control of their authorized project manager.

3.5.1 Data and Infrastructure Monitoring

3.5.2 Collaboration with Third-party Vendors

3.6 Data Security Officers

3.7 Security Breach Response

3.7.1 Security Breaches

3.7.2 Enforcement Sanctions

Summary

The GreenTrax security application was designed to develop, test, and document a well-structured and easily understood coterie of processes and sub-applications that will assure the management and access of GreenTrax generated data throughout the several coordinating layers of the user interface, background IT systems, as well as the chain of custody of the data when used by other segments of the enterprise. Each aspect of the security application as a whole—L1Sec, L2Sec, and L3Sec—work together to provide the level of security required to maintain the integrity of the end-user's access to the system, the data exchanged, and to enforce the exclusion of unauthorized access to the system along its many vectors of attack by potential data security threats. Misuse of the data is also a concern, and is addressed by this security application. All these layers and considerations are contained with the GreenTrax security application.