ImPACT Applications Security

ImPACT Applications has implemented many policies and procedures as it relates to the security, privacy and availability of our application environments. We undergo annual SOC 2 Type II audits by an independent third-party auditor covering the domains of security, privacy and availability. ImPACT Applications has also achieved ISO 13485 certification for our quality management system. Below are the highlights of many of our policies, outlining the steps we take to make sure our environments are safe and secure.

Datacenter Information

Security

ImPACT Applications uses a colocation datacenter facility to house our equipment. The facility has completed an SOC 2 Type II audit. It employs state of the art access control systems. Entry to the building and to various other sections of the facility including the computer room are controlled by a multi-factor access system, requiring a key card, a pin code, and a fingerprint scan for entry. All external doors, as well as the computer room floors are under 24x7x365 video surveillance. Motion detection and alarms are used during off-hours. Guest access is logged, and guests are escorted throughout the facility by datacenter staff.

Physical

The datacenter, a tier 3 facility, uses fully diverse electrical paths for power from the outside utility through to the customer cabinets. Redundant UPS units provide short term power protection to all systems in the datacenter, while redundant diesel generators provide long term power protection, with enough fuel for 36 hours of constant running at 100% load. A fueling contract is in place as well, to ensure uninterrupted power in the event of a major long-term outage.

The facility provides redundant network paths using 7+ ISPs and BGP routing to ensure maximum network availability. We also have redundant firewalls, switches, and bonded network interfaces in our servers to ensure that there is no single point of failure in the network path.

The HVAC system at the datacenter is an N+1 configuration, with a spare unit rotating into service monthly. A maintenance contract is in place, providing routine checks and cleaning to ensure the equipment is functioning to its fullest potential, and prevent any unexpected problems.

Fire suppression is accomplished through a conventional smoke and heat detection system and a pre-action dry pipe sprinkler system. Clean agent fire extinguishers are also located throughout the facility.

Application Security

Field validation

Input fields throughout the application are checked and validated for appropriate format to ensure that correct information is provided by the end user. This helps to ensure that proper information is received, stored and reported upon. Also, this ensures that only expected data is transmitted, helping to thwart any attack attempts made through input fields.

Database encryption

All fields in the database that store personally identifiable information are encrypted using AES-128 bit encryption.

Data in-transit encryption

All data transmitted between the end user's computer and the ImPACT Applications systems is encrypted using the highest supported encryption method of the end-user's web browser. A minimum of 128-bit encryption is required. Any request made over an unencrypted channel (HTTP) is automatically redirected to an encrypted channel (HTTPS) before it is allowed to complete.

Access logging

All access to protected health information is logged by our application. This includes reports that are generated, modifications or corrections to PII that are performed by the user, and any data that is requested to be exported from the system. Access logs are written in a date/time stamped format identifying the user that performed the action, and the details of the action that they had performed.

Session timeout

The ImPACT Applications Customer Center utilizes a 20-minute idle timeout to prevent unauthorized access. Additionally, if a user administers a test through one of the links inside of the Customer Center, their session is immediately logged out upon the start of that test to prevent the test taker from being able to exploit the open session.

Account information

Access to the ImPACT Applications Customer Center is accomplished through unique username/password authentication. Each user of the system receives their own account, and we do not limit or restrict the number of accounts allowed per customer. The application uses the following role structure to allow customers to allocate permissions in a least-access manner.

- System Management Only
- Baseline test administration only
- Baseline and Post-Injury test administration
- Baseline test administration and access to baseline results
- Baseline and Post-Injury test administration and access only to baseline results
- Baseline and Post-Injury test administration and access to all results
    - System Management permission is able to be granted in conjunction with any of the above permission levels.

Users are associated with one or many organizations inside of the system. Users are only allowed to view or retrieve data from those organizations that they are associated with and have valid permissions to.

Operational Security

Database backup and encryption

The database behind the ImPACT Applications system is backed up hourly. The backup files are encrypted using AES-256 encryption prior to being transferred from the database server to any other storage location. The backup files are stored in three locations, two are geographically separate from the production infrastructure. Each backup is logged, and system administrators are notified when a job has occurred along with the detailed result of the backup job.

Server installation guidelines

Our systems are installed with a CentOS "minimal" install. We have a base install build sheet that all of our servers are configured to, which sets up our initial user accounts, basic software and services common to all systems, and the like. From there, we have specific build sheets based on the type of server that are followed. For example, one for database servers, one for a particular type of web server, etc. This ensures uniform configuration for all systems in our environment and serves as a checklist so that we are sure they are all built to the same specification.

Network vulnerability assessment

We perform quarterly network vulnerability scans against our environment. Any vulnerabilities discovered as part of these scans would be assessed for validity and severity. Items requiring correction would be addressed as part of a corrective action item.

System patch management

ImPACT Applications system administrators monitor several notification lists from our software vendors to remain informed of critical issues. Any

remotely exploitable critical bug or security issue is patched as soon as possible, usually within 2 days of receiving notification, to eliminate the potential risk presented by the issue. Patches that are non-critical, or not remotely exploitable are applied on a quarterly basis, starting with our development environment, then QA, and finally after the patches have proven effective and not harmful to the function of the application, they are applied in production.

Production system access review

Annually, and also if/when any modifications to the user lists are made, we review the active accounts and access levels of our production systems. We will gather together the list of active users on the servers and VPN devices, along with a list of accounts with elevated privileges, ensure that all are valid, and make any adjustments necessary to ensure no invalid accounts are active, and all accounts have the appropriate levels of access. This is supplemented by policies that are followed when employees join or leave the company to ensure that access is approved when granted and revoked when no longer needed.

Service outage and security events

In the event of a service outage or security event, ImPACT Applications has a defined policy to ensure that a root cause is determined, documented and remediated by whomever the responsible party is. These documents are filed when an issue is detected and amended throughout the discovery and remediation process. Notification in the event of a data breach is also part of this process, and the proper notification processes will be followed according to applicable law. After all steps have been completed, and any remediation steps have been completed and verified, the document will be closed and filed.

Network layout

ImPACT Applications uses a web application firewall (WAF) to protect the application from malicious attack attempts. The WAF in place defends against OWASP Top 10 threats, including SQL injection, cross-site scripting,

illegal resource access and remote file inclusion. Using advanced client classification technologies, the WAF is able to distinguish between "good" and "bad" bot traffic, allowing us to block scrapers, vulnerability scanners and others, while allowing other legitimate services to access the site. The WAF also monitors website traffic to prevent backdoor install attempts and to quarantine backdoors that are already installed, rendering them useless. The WAF also allows us granular control to be able to block whole countries, specific bots, IP addresses, or URLs. DDoS protection is also provided by the WAF.

The server network is arranged in layers, each layer a DMZ to itself with only necessary access between them. The systems are protected by a redundant pair of firewalls. Traffic is then passed through to a redundant pair of load balancers, then allocated to one of many web servers to handle the request. The web server will request information from the database layer, and then formulate a response back to the end user. Only appropriate ports are open between the DMZ to reduce risk and limit lateral movement in the event of a system compromise.

Access is permitted to our production environment for ImPACT Applications system administrators only. No developers or testing personnel have access to the production systems. Our infrastructure is structured such that access can be allocated to a particular set of servers in any of our environment to a defined user class.

ImPACT Applications uses an OpenVPN device to provide remote access to the datacenter environment for users that require access. The OpenVPN is configured with role-based access rules to allow users access to only the systems that they require access to in order to perform their duties. Developers only have access to development systems and QA personnel only to QA systems, while system administrators can access all servers.

ImPACT Applications employees are required to use a two-factor authentication system to log into the OpenVPN. In addition to a username and certificate, remote users must provide a second authentication token,

either a passcode or acknowledgement of a notification to a pre-registered device (smartphone or hardware token).

Monitoring

ImPACT Applications uses Nagios primarily to monitor our systems. We monitor as many available data points as possible, as appropriate for the type of system being monitored. Standard monitors include CPU usage, Memory usage, Load, Disk usage, NTP status, and several others. System specific monitors include HTTP connection counts for web servers, web server status, database performance items, etc. Each monitor has a defined range. If a monitor detects that a check is out of range (high CPU usage, for example) ImPACT Applications system administrators are notified of the condition. Each of our sites has its own Nagios instance, and because of this we are able to also monitor the sites availability, as well as other items like SSL Certificate expiration.

ImPACT Applications uses a package called pnp4nagios to store and provide trending data from Nagios. We use this information to evaluate server performance, identify peak load times, and plan for future infrastructure expansion. We gather snapshots of the production infrastructure's performance monthly and evaluate for any increased loads or other items that would require additional resource allocation.

ImPACT Applications also makes use of NodePing, a monitoring service that checks our various websites from locations around the globe to ensure uniform availability from a vast set of locations. We have NodePing check a particular test page that exercises the full application stack, ensuring that all layers are checked as part of the test. In the event of an error, NodePing will send e-mail and text messages to ImPACT Applications system administrators.

ImPACT Applications has installed a host-based intrusion detection system (HIDS) on all of our servers. The HIDS monitors log files to watch for errors, keeps checksums of critical system files and evaluates for unexpected

changes regularly, and also monitors for new or updated software packages on the servers. If any anomalies are found, ImPACT Applications system administrators are notified of the condition.

Disaster recovery

ImPACT Applications has a hot standby disaster recovery environment. All systems at the DR facility are online, running the current production version of application code, are fully monitored, and ready to assume the production load. A disaster recovery plan is documented and tested annually. Database backups are automatically copied from our production facility to the DR facility hourly.

Testing our DR environment requires simply restoring a backup copy of our production database to the systems in DR, accessing the site through an alternate URL, and running through a scripted set of actions to verify that the site is fully functional.