

# BSDI Security Policies and Procedures for the Motivation<sup>®</sup> Web Application

Document Last Revised: 21 October 2009

Author: Dr. Mark Brittingham (Mark@BSDI.cc)

Revisions and/or Suggestions to: Andy Aron, BSDI Technical Support ([Andy@BSDI.cc](mailto:Andy@BSDI.cc))

---

## Introduction

The purpose of this Security Policy Documentation is to capture the policies, procedures and personnel responsible for ensuring that BSDI's Motivation Web Application and the associated data entrusted to BSDI by our clientele are protected from unauthorized access, are shielded from attempts to intercept, corrupt or destroy such data, and are protected against loss from hardware failure and/or natural disaster.

The Motivation Web Application collects, processes, stores and interprets a wide variety of data including some quantity of Protected Health Information (PHI). U.S. law (HIPAA) and BSDI policy require that all data, including PHI, be secured so that only those personnel authorized to view the data have access to it. "Authorized personnel" includes the professional health promotion staff tasked with using this data to assist in the development of programs and materials for participants as well as the participants themselves as they access their own, and only their own, PHI.

## System Description

Motivation is an ASP.NET 2.0 Web application running under IIS 6.0 on one of BSDI's Windows 2003 or 2008 Web Servers and accessing a Microsoft SQL Server 2005 database running on a separate Windows 2003 Server. All of BSDI's web sites store data on only BSDI's database servers.

BSDI hosts all of its Motivation sites with MaximumASP – a server hosting and management company located in Louisville, KY. MaximumASP manages BSDI's servers as well as the networking equipment, system backups, logical security perimeter (firewalls, etc.), network connectivity, facility power, temperature and humidity control systems, fire suppression systems and physical security. Much of the security footprint (i.e. the physical and logical network) that BSDI offers is actually provided by MaximumASP. This document will briefly describe the security offered by MaximumASP but the reader is encouraged to review the information at: <http://www.maximumasp.com/infrastructure/security>.

## Security Requirements

Motivation offers participants a data management tool for recording health risk assessment responses, medical status information, exercise-related activities, weight, blood pressure, exercise plans, fitness testing results and other health and wellness information. Our primary security requirement is that this information be available to the participant and to the duly appointed professional staff managing the participant's wellness program and yet be resistant to attack, discovery, or corruption by any agent outside of these two entities.

There are three primary vectors for attack against a Motivation web site: frontal or technical attacks in which an outside entity attempts to penetrate the database and/or web site using technical means (e.g. discovering a security account capable of accessing SQL Server, executing a cross-site scripting attack), “inside” attacks in which a staff member attempts to inappropriately access private health information, and ‘social’ attacks in which an outside or inside entity induces a participant or, more critically, a professional staff member to reveal enough information to permit them to access the site.

BSDI defends against these attack strategies by reliance upon our Security Design and Management Plans.

## Security Design and Management Plans

### Technical Attacks - MaximumASP

The Motivation system anticipates and defends against technical attacks by pursuing a variety of strategies. The most fundamental strategy is simply to partner with strong, security-minded company in MaximumASP. This partnership, for example, ensures that all of our servers receive and install the latest security patches to Windows Server, IIS and SQL Server as Microsoft releases them. In addition, MaximumASP offers a robust and multi-layered security architecture including intrusion prevention systems (IPS) to detect and block exploits, attacks, reconnaissance attempts and other unwanted traffic. As per the MaximumASP documentation: “In most cases when a vulnerability or exploit is released, it takes our IPS vendor approximately 3 hours to write and release a signature to stop these attacks.” The MaximumASP IPS:

- Detects and deflects attacks and intrusion attempts.
- Provides network-based anti-virus scanning.
- Uses traffic anomaly algorithms to detect and block zero hour attacks even before specific OS and application vulnerabilities are known.
- Receives automatic distribution of latest exploit/attack signatures.

MaximumASP also maintains edge layer firewalls to protect the MaximumASP network from the public Internet. All of BSDI’s servers operate within MaximumASP’s network and have enterprise anti-virus software installed and managed by MaximumASP. BSDI’s Motivation database servers are also fully insulated from the Internet via a dedicated hardware firewall that permits access only from BSDI’s web servers. Thus, no direct attack on the SQL Server databases via the Internet is possible.

Finally, MaximumASP offers physical security including 24/7 monitoring, biometric access to the physical plant, a CCTV monitoring system, and a physical alarm. They also enforce zoned access and use security glass and reinforced doorframes, walls and ceilings at all access points. They offer complete data center systems redundancy including zoned cooling, power, and fire suppression systems. MaximumASP and BSDI are “Business Associates” for our clients as the term is defined and used in HIPAA. MaximumASP does not access the underlying database other than running automated backup utilities. BSDI will access the database only to perform maintenance or to response to information requests from approved staff at the client’s site.

### Technical Attacks - BSDI’s Security Strategies

BSDI provides our Motivation clients with a 128-bit SSL certificate to secure their Motivation web site. This ensures that all traffic to and from the site is fully encrypted.

Motivation has been subjected to a SPI Dynamics WebInspect Vulnerability Audit (2007) and an IBM WatchFire Vulnerability Audit (2009) and the findings were particularly encouraging. After the original WebInspect Audit, we were informed that Motivation was the first application ever audited by our SPI Dynamics team that was fully secure and impenetrable from the outset (SPI Dynamics is now a subsidiary of HP). That is, no security changes were required as a result of this audit: reflecting BSDI's strong commitment to secure computing and ability to deliver it.

Similarly, Motivation passed the WatchFire audit with an outstanding score: only one possible vulnerability was found out of over 200,000 automated tests (99.999995%). The reported WatchFire vulnerability was manually checked and found to be on the administrative interface (where hacking is hardly relevant given that administrators have full access anyway) and harmless in any event (no exploit was possible – a false positive). Motivation was altered to remove the false positive after the audit was completed.

BSDI's production database servers and the data they hold have been hardened in a variety of ways. First, the database servers are visible only to BSDI's web servers due to its sequestration behind a dedicated hardware firewall. Next, each Motivation web site is associated with a dedicated database on our server rather than sharing data with other Motivation web sites. Thus, no error in SQL retrieval, for example, could ever reveal one organization's data to another organization. The production and development database servers are completely separate and no development work is done against the production database server.

Next, the "sa" account on our SQL server has been disabled so there is no SQL-based administrative account available to an attacker even if they were able to gain access to the server. Note that the SQL server accounts and passwords used by BSDI are not provided to clients; they are for internal use only.

The SQL Server account passwords that govern access to the database server are subject to SQL Server's built-in password complexity standards and, indeed, are quite a bit more complex than even the Microsoft SQL Server standards require.

BSDI's internal development and support computers are secured from physical and network threats in a variety of ways. BSDI uses firewall/spyware/anti-virus software as well as a physical firewall to protect our network from the Internet. BSDI uses dedicated development machines (physical or virtual) for all internal development. These development computers never access email or web sites other than those managed by BSDI or BSDI's tools providers (e.g. Microsoft). This helps ensure that no outside malware can make it on the development platform.

All internal documentation regarding server passwords or other sensitive information is maintained in an encrypting database utility which uses a 448-bit 'blowfish' algorithm to encrypt this information so that it remains hidden even if someone were to gain physical access to a BSDI computer.

No laptops or other portable computers or devices are permitted to access the MaximumASP servers or any aspect of the development environment.

Only two of BSDI's employees have access to the MaximumASP servers and both have worked at BSDI for over a decade (Dr. Brittingham and Mr. Aron). That is, access is reserved for those with a strict "need to know." All of BSDI's employees are required to maintain complex passwords to guard their computers and are forbidden from storing passwords for their computers or for customer web sites in non-encrypted files or on physical media (e.g. no "sticky notes" or notebooks with sensitive passwords). As a matter of policy and practice, Motivation client databases are never downloaded to media at BSDI's home office except A) in the event that the database is to be shipped to the client at the end of a contract or B) at the request of the client for testing or analysis purpose.

Our clients' web sites also feature the use of staff accounts that have access to PHI. As detailed below, we expect these accounts to be maintained by the customer according to the same standards maintained by BSDI.

## Security Management Plan

### Access Management – Preventing Inappropriate Access

Participants in a Motivation health promotion program may enter Personal Health Information (PHI) into the system. As dictated both by law and common sense, the only entities to whom access to this information should be given by a service provider are the participant and the caregivers to whom he or she has given either explicit or implicit consent. Consent is given during system enrollment when the participant signs the electronic Consent form that begins the enrollment process.

To help safeguard private data, Motivation employs an *Access Management* strategy. Access Management has three components: preventing unauthorized visitors from logging in to Motivation, preventing one participant from seeing another participant's data, and preventing unapproved staff members from accessing Private Health Information (perhaps due to being at a different location).

### Preventing Unauthorized Access

To prevent unauthorized access to Motivation, the software requires a visitor to log in with an ID and password. Motivation also forbids all access to the bulk of the site to anyone who has not logged in (the only exceptions being the library articles, about page, privacy policy, calendar, login and account creation pages). We use the "forms authentication" mechanisms built in to ASP.NET to provide this access gating. This prevents, for example, anyone from simply typing in the name of a page within the system to access that page.

As a matter of policy, all staff members must have their own, individual set of login credentials. The sharing of login credentials is strictly forbidden. Staff passwords are required to meet minimum complexity requirements (6+ characters, at least one uppercase character, at least one non-alpha character). The participants may or may not be required to use complex passwords: this option may be enabled or disabled via the configuration screen.

### Preventing Participants from Viewing Each Others' Data

Preventing participants from seeing one-another's data is primarily a matter of simple software design. For example, when a participant attempts to retrieve any page containing PHI, Motivation does not rely on URL arguments or a client ID stored in a "cookie" to select records. Instead, Motivation uses internal session data to ensure that the data being requested is specifically associated with the logged-in participant. Internal session data is identified by a "session cookie" that is so long and complex that there is essentially no possibility that a hacker could guess another session's identifier (120 bits). We thus prevent all attempts to "game" the system by the use of URL arguments, the manipulation of the HTML GET parameters and even manipulations of the session cookie. None of these approaches will result in a compromise of PHI.

Cross-site scripting attacks, wherein a client will attempt to "hijack" a page on the site to expose the information for other visitors is defeated by the use of input (form and URL) filters that prevent the entry of scripts and/or HTML. As discussed below, security audits have found that Motivation cannot be penetrated by the use of cross-site scripting.

The only case in which participants can see one another's data comes when they are participating in team events (e.g. the Team Lean Challenge – participants can see how much weight their teammates

have lost). In this case, participants joining the program have the opportunity to use an “alias” instead of their real name. While this option is essentially never used in practice, it serves to underscore the degree of privacy available to participants.

### **Preventing Unauthorized Staff Access to Participant Data**

With respect to staff access to participant data, Motivation offers a multi-tier system of access that permits the organization to limit access to data in a variety of ways. First, staff members may be forbidden from having access to any personal data even if they otherwise have a system login (e.g. to manage the calendar). That is, staff accounts must specifically be given member services privileges before they can access any participant data. Second, even among staff members having access to the member services area (holding client information), privileges to view PHI can be withheld. This is useful, for example, when some staff only access participant records for membership management purposes. Thus, the only staff that can see PHI are those that a) have a login, b) have access to member services and c) those with specific rights to view PHI. In addition, it is possible to limit a staff member’s privileges to only a single *Location* within Motivation. Thus, for example, an organization with facilities in Chicago and New York might limit the Chicago personnel so that they can access only the data for participants in Chicago – and not be able to see data for those in New York.

In addition to these tools, Motivation also provides a “high-privacy” mode in which participants can forbid all access to their PHI without their specific, temporary permission. That is, if a staff member needs access to a participant’s PHI, the participant must be present and willing to enter their password into Motivation. When they do, the staff member will have access to the participant’s PHI only until they exit the software or access another participant’s record.

In addition to these strategies, all staff access to participant records is logged (Version 12 only). The access logs cannot be changed from within the Motivation user interface.

### **Education and the Limitations Social Attack Prevention Strategies**

One must never forget that BSDI’s only real mechanism for preventing a social attack is to educate the professional staff at our customers’ facilities about the need to avoid revealing their login information and/or other sensitive information to anyone. However, there is very little we can do to prevent penetration of the system if professional staff, or the participants themselves, do not take steps to preserve the privacy and integrity of the data. When a site is brought up for a client, BSDI provides one or more “staff” accounts to the client so we have a “teachable moment” in which to drive the security message home. However, after this point, the primary administrative contact can create additional staff accounts or can simply share one or more staff accounts against our wishes and instruction. Once they’ve begun managing their own data, we must trust in the good sense of the user to avoid compromising the security infrastructure that we have constructed.

## **Backups and Disaster Recovery**

### **Database Availability and Backup Policies**

BSDI maintains all databases on a SQL Server 2005 Standard installation running on a MaximumASP quad-core, 2GB server. The databases on this server are backed up to an identical, SQL Server-equipped server each night so that, even in the event of a complete hardware failure, customer data will remain safe and accessible. That is, if the primary server should fail, the backup server can restore existing customer databases and begin serving data requests within a few hours. Depending on your service

level agreement, BSDI may also provide a “log-shipping” arrangement that minimizes total data loss by taking more frequent snapshots of your database and storing them to the backup server.

Note that the database backups are all encrypted using a 256-bit encryption algorithm so that anyone coming into possession of them could not restore the data.

## Data Lifecycle

The database backups are kept for 5 days on the backup database server. No temporary physical media is used to store client data and so no issues related to the destruction or shredding of documents or CDs is raised. Note that off-site storage of customer data backups and failover clustering of database servers is available for an additional fee.

## Disaster Planning

With respect to our disaster recovery plan, we foresee three primary threats to our business continuity: temporary power outages, natural disasters that result in destruction of business property and data, and electronic penetration of our network and theft/destruction of electronic property.

All three primary threats are somewhat mitigated by our reliance on the robust infrastructure provided by MaximumASP for our client data and web site management. For example, MaximumASP uses redundant power supplies (including on-site generators), multiple connections to the Internet provided by different vendors, etc. as detailed above and on their site. In the event that any of the threats described above occur BSDI’s home office, BSDI’s core business would not be affected. Of course, our ability to update sites and to monitor their performance is still quite critical and we would indeed need to bring the business office back online as soon as possible.

Temporary power outages are a low-level threat to BSDI’s business. They take out our ability to access our MaximumASP servers from the office and disrupt our phone service. To deal with server access, one employee (Dr. Brittingham) has a duplicate environment at home that permits full access to these computers. This computer is fully password protected and all business data is maintained in a fully encrypted “Data Guardian” database – just like the computers at work. Thus, in the event that the office is disabled, we are generally able to access the MaximumASP servers (the exception being a widespread power outage that takes out both areas).

Phone service outages would be handled via our ability to forward phones to the home offices maintained by four of our employees (with the exception mentioned above, the home offices do not have access to private customer data on the MaximumASP servers).

With respect to the destruction of business property and/or data, there are two classes of data that are our primary concern: the source code of the products and the business documents and accounting data.

BSDI makes use of an externally managed source code repository to store the Motivation source code and supporting materials. We also maintain a library of software tools so that, in the event of a disaster, we can restore our development environment in the time needed to purchase new computers, install the necessary tools from our library and restore the source code from backup.

Business system backups (e.g. accounting) are made every evening by copying from our accounting server to another server in the office. On a weekly basis, backups of these systems are made to CD-ROM and then stored in a 450 lb vault maintained off-site and down a flight of stairs. Such backups include all of the essential information needed to ensure that the business can survive in the event of a catastrophic loss of our physical facilities.

With respect to electronic attacks, we have a multi-layered defense to mitigate risk. BSDI's offices feature a hardware firewall as well as software on the computers to prevent malware infections. All computers are kept up with the latest patches from Microsoft and Apple. As mentioned above, developers use separate computers for development and for web/email access in order to avoid any compromise of the source code. Finally, all sensitive customer data (e.g. access passwords for our MaximumASP servers) is strongly encrypted in a "Data Guardian" database so that, even if a hacker gained control of a computer, they would not be able to discover these passwords, etc.

In the event of a network penetration, the worst-case scenario would involve clearing all computers and "rebooting" the business from our data backups.

## **BSDI Personnel and the Management Plan**

BSDI is a small company with a traditional focus of client service. The primary agent responsible for the day-to-day management of security in the company is our technical support engineer, Andy Aron. Mr. Aron acquires and installs SSL certificates, enforces password policy, administers user and SQL Server accounts, secures and verifies the encryption of sensitive data, and works with our clients to help them understand their responsibilities under HIPAA to manage their data safely.

Suspected security incidents are also reported to Mr. Aron. He is charged with logging such incidents, analyzing the nature of the incident and the data that may have been compromised, notifying any affected parties, and making appropriate changes to the passwords, network configuration or other resources affected or coordinating with MaximumASP to do the same.

The primary agent responsible for planning BSDI's overall strategy for managing the Motivation software throughout the life cycle of each release and for ensuring that our client's enjoy robust security for their data is Dr. Mark Brittingham, BSDI's president and CEO.