DDI Security Policy

It is the policy of DiscipleData to proactively safeguard all aspects of our technical infrastructure, systems and services from unauthorized access, alteration or destruction.

The following elements of this policy are intended to:

1. Protect DDI's systems, data, and intellectual capital (IC)
2. Protect client data from unauthorized access.
3. Ensure that DDI's systems are always secure
4. Ensure that DDI's security meets external control audit requirements.

Responsibilities

- DDI management is responsible for maintaining, implementing, communicating and measuring the compliance of the DDI Security Policy.
- All DDI Staff are responsible for understanding and following the DDI Security Policy, as well reporting anything they feel violates the policy to DDI management. DDI staff should also suggest enhancements to the policy as they are recognized.
- DDI clients have responsibilities with respect to the DDI Security Policy as outlined in this document.
- DDI communicates this policy to clients and requests their cooperation and compliance with all applicable sections.

DDI management may revoke any approvals outlined in the DDI Security Policy.
The DDI Security Policy will be reviewed at least annually, or when changing conditions warrant a review. This policy will be updated as necessary to incorporate provisions determined through periodic reviews. Revisions will be communicated in writing to DDI staff and clients.

System Software Versions, Updates and Patches

All systems must be kept up to date with respect to system security. Security related updates must be installed as soon as is practical on applicable servers and workstations.

System Environment Safeguards

DDI maintains hardware appliances and software to prevent security violations. Safeguards will be applied and maintained at appropriate levels.

System Administration Authority and Responsibility

DDI management will grant system administrations authority to specific individuals only. It is understood that system administrators have complete control and many things they access and change under the direction of management. There is an intentional division between software development personnel and operations personnel with respect to production system access levels. Management may be granted system administration authority.

Administrators must log all changes to system and environment configurations along with the reasons for the changes to a central system update audit log. There must be at least two administrators fully trained on each DDI system and service. System administration passwords (current and all previous) are maintained in a software utility that stores information which is strongly encrypted with a master password. The encrypted password file is available to authorized system administrators. It is also kept in a container at the offsite storage facility.

Any loss of a system administrator requires an immediate and comprehensive change of all passwords for service accounts with domain admin authority, an update of the master password, and an update of the offsite storage container. Passwords are not to be kept in writing, in any location other than the offsite storage container.

Account and Password (Credentials) Administration
Accounts and passwords are used to control access to various systems. A user should have common credentials across multiple systems wherever feasible. The use of generic accounts must be approved by DDI management.

Accounts will be either disabled or deleted as defined below upon notification by client or DDI management. Disabled accounts must be reviewed periodically and deleted when no longer required. Accounts must be reviewed and updated periodically with clients. In all cases, user administration changes, including password resets, must be logged. Limited aspects of user administration may be delegated to client personnel with the mutual approval of DDI and client management.

Security Requirements

- Regular password changes with complexity rules will be enforced.
- Accounts will be temporarily locked out upon successive password failures to protect from automated credential cracking attempts.
- Initial password assignments will require immediate change by the end user upon their first use.
- Users must be able to change their password themselves at any time.
- Passwords communicated to a user (by phone or email) must be a one-time use password that the user will be forced to change upon first use. Passwords must not be sent to anyone other than the end user via email, unless their supervisor requests it
- End users will never be asked for any passwords by DDI staff.
- Only a DDI management is authorized to issue anyone a system administrator level password. Any issuance of a system administrator level password must be documented in the user maintenance log .

External System Access
Firewalls must be set up with explicit ‘allow’ rules and all other traffic denied. No traffic should be implicitly allowed inbound. All public servers will use SSL to encrypt public communications.

Multi-layer security should be implemented wherever possible and practical.

Monitoring, Reporting and Auditing
All production equipment and services will be monitored internally at all times. Reporting of failures will be via email and SMS text messages to the entire data center staff, with complete history maintained.

Centralized auditing with history, regular reports and alerting capabilities will be enabled to the fullest extent practical on all systems. Important audit logs must be regularly reviewed.

Data Protection
Each DDI client has exclusive access to their organization's data only. Client data must be rigorously protected from other internal and external users. DDI staff, other than system administrators and support staff, should not have direct access to production client data or production client backups. Programmers may be given temporary read only access to client production data by support staff only for purposes of troubleshooting a client problem or request. Sensitive data (SSN, credit card info, birthdates, etc.) must be encrypted including on backup media of all types. Important data is stored using SAN technology and replicated between data centers.

Physical Security
All DDI data center locations will be physically secured by access control methods which allow individual access credentials and maintain access logs. All server consoles will remain logged off or have a password protected screen saver invoked at all times.

Development System
Authorized DDI staff will be given complete access to development systems, provided these systems do not contain production data.