Terra Dotta Information Security Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	14 Jan 2015	Initial Policy	Garrett Christian Scott Burkett	Garrett Christian
1.1	20 July 2015	First Policy Review	Garrett Christian Scott Burkett	Garrett Christian
2.1	22 Jan 2016	Annual review	Garrett Christian Scott Burkett	Scott Burkett
2.2	14 July 2016	Mid-year review	Garrett Christian Scott Burkett	Scott Burkett
3.1	09 Jan 2017	Annual review	Garrett Christian Scott Burkett	Scott Burkett
3.2	11 Jul 2017	Mid-year review	Scott Burkett	Scott Burkett
4.1	18 Jan 2018	Annual Review	Garrett Christian Scott Burkett	Scott Burkett
4.2	26 Jun 2018	Semi-annual Review	Scott Burkett	Brendan Haggerty
5.1	08 Nov 2018	Annual Review	Scott Burkett	Brendan Haggerty
5.2	09 May 2019	Semi-annual Review	Scott Burkett	Brendan Haggerty
6.1	12 Nov 2019	Annual Review	Scott Burkett	Brendan Haggerty

Introduction

The security Terra Dotta's and our clients' sensitive information and environments where sensitive data exist are the highest priority of the company, as any threats to that information could jeopardize both the safety of our clients and the future of the company itself. The following security policies have been developed to protect Terra Dotta critical operations, partners, assets, employees and customers. Compliance with these policies is mandatory. If you have any questions regarding any of the policies or your responsibilities in implementing them, please contact the Information Security Officers (infosec@terradotta.com).

Terra Dotta shall comply with the provisions of all applicable privacy statutes and regulations and protect against unauthorized access or use of sensitive information. Furthermore, Terra Dotta is committed to maintaining compliance with the Payment Card Industry Data Security Standards (PCI DSS) both in recognition of our responsibility as a service provider with functional links to payment gateway services and as a basis for strengthening our security practices on the whole. PCI DSS is well recognized as one of the most comprehensive and intensive standards in existence, and we regard it as an excellent framework on which to base our practices. While Terra Dotta's systems and proprietary software do not--by policy and by design--transmit, process or store any PCI cardholder data, we are using the standard to guide our treatment of all other types of sensitive information/data and the environments where sensitive data exist.

This Information Security Policy describes safeguards to protect sensitive information of Terra Dotta (the “Company”) and its clients.

These safeguards are provided in order to:

- Protect the security and confidentiality of sensitive information;
- Protect against anticipated threats or hazards to the security or integrity of sensitive information; and
- Protect against unauthorized access to or use of sensitive information that could result in substantial harm or inconvenience to Terra Dotta or any of its clients.

Terra Dotta recognizes that both internal and external risks exist. These risks may include:

- Unauthorized access of sensitive information by someone other than its owner
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Unauthorized transfer of sensitive information through third parties

This may not be a complete list of the risks associated with the protection of sensitive information. Since technology growth is dynamic, new risks are created regularly and must be protected against.

Distribution

This policy is to be distributed to all groups and individuals with access to Terra Dotta systems, which includes all Terra Dotta employees, consultants, partners, and/or other staff members.

The most current version of this policy is to be readily available and accessible in the Terra Dotta Internal Share: Security Policies folder on Google Drive (TDIS). All referenced documents within this policy and it's linked sub-policies and procedures are found in the same area of the Terra Dotta Internal Share.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Terra Dotta Chief Technology Officer (CTO) for review and approval using a Change Request Form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

This policy will be reviewed every 6 months. The next scheduled review date is the week of 11 May 2020 by the Systems Architect, to be approved by the Terra Dotta CTO.

Policy

Definition of Sensitive Information for the purpose of this policy includes:

- Any data that is protected under the Family Education Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), or the Health Insurance Portability and Accountability Act (HIPAA).
- Cardholder data, as defined by PCI DSS 3.2, namely the PAN (personal account number), PIN (personal identification number), or CVV (card verification value).
- Any data created by the institution or the institution's users that is not otherwise obtainable from publicly available information, or from federal, state or local government records lawfully made available to the general public.
- Proprietary information of Terra Dotta which includes, but is not limited to, the terms of client agreements; the structure, design, algorithms, data structures, logic flow, and screen displays associated with Terra Dotta Software; Terra Dotta documentation; and Company pricing, sales and training materials.
- Terra Dotta also chooses as a matter of policy to define covered data to include any information of such a nature that a reasonable person would understand such information to be confidential. Sensitive information includes both paper and electronic records.

Other Definitions:

Availability Ensuring that information systems, data and network resources are available and ready for use when they are needed.

Confidentiality The protection of data from unauthorized disclosure.

Consultant A non-permanent employee, or a person contracted and paid through a third-party.

DMZ Demilitarized zone. Network added between a private and a public network to provide an additional layer of security.

Employee A full- or part-time employee hired directly and on a permanent basis, as well as contracted employees hired directly or through a staffing agency to serve as members of the Terra Dotta staff.

Emergency Change A change which, due to urgency or criticality, needs to occur outside of the Terra Dotta's normal change management process.

Encryption Process of converting data into an unintelligible form except to holders of a specific cryptographic key.

Information System Information systems include, but are not limited to, laptop computers, workstations, servers, mainframe computers, routers, switches, mobile phones, tablet computers, telephones, fax machines or other devices that handle data.

Integrity The accuracy, completeness and validity of information.

Logical Controls
Controls that limit access to information systems and/or data at the electronic level. For example, passwords, user accounts, firewall rules.

Malicious software (Malware)
Software designed to damage or disrupt information systems, data, or network resources.

Network Resource
Communication links and network bandwidth.

Partner
An organization or individual contracted with Terra Dotta to serve in a fully transparent relationship, under legally established non-disclosure agreements and signed agreement to follow all Terra Dotta security policies and procedures.

Physical Controls
Controls that are implemented to restrict physical access to systems infrastructure. For example, surveillance cameras, motion alarms, door locks, security guards.

Risk
The likelihood of a given threat exercising a particular potential vulnerability, and the resulting impact of that adverse event on an organization.

Security Incident
The attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or services used or provided by the Terra Dotta.

Strong Cryptography
A cryptographic algorithm or protocol that makes it very difficult for an unauthorized person to gain access to encrypted data.

Threat
Condition that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the Terra Dotta.

Multifactor Authentication
The use of two or more independent types of mechanism for authentication. For example, a security token and a password. Also known as MFA, or 2FA (for two-factor authentication).

User
Anyone who accesses Terra Dotta information systems, data or network resources.

Visitor or Guest
A vendor, guest of an employee, service personnel, or anyone who needs to enter a Terra Dotta facility containing information systems, data or network resources for a short duration, usually not more than one day.

Roles and Responsibilities

Responsibility for information security on a day-to-day basis is every Terra Dotta employee's duty.

Terra Dotta has designated its Chief Technology Officer to be its Information Security Policy Coordinator (the "Coordinator") and to be responsible for the Information Security Policy. The Coordinator will provide guidance for compliance with Company security policies. The Coordinator or his/her designee will assist the Company to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of sensitive information: developing and maintaining necessary policies and procedure; regularly reviewing and evaluating the effectiveness of the current policies and controls; coordinating security reviews and audits.

Specific guidance, direction, and authority for information security is the responsibility of Terra Dotta's Information Security Officers, which are the CTO and the Systems Architect. Accordingly, the ISOs will conduct and/or oversee the following activities:

- Maintenance and distribution of information security policies, standards and procedures.
- Monitoring, analysis and distribution of security alerts/information to Terra Dotta employees.
- Maintenance and distribution of the Incident Response Plan and associated escalation procedures.
- Administration of user accounts, including additions, deletions, and modifications.
- Monitoring and control of all access to sensitive data environments.

Current Officers (as of January, 2017):

- Brendan Haggerty, Chief Technology Officer
- Scott Burkett, Systems Architect and Information Security Officer

Reference: PCI DSS v3.2 requirement 12.5 (12.5.1 – 12.5.5)

Employee Management and Training

All Company employees are required to sign a Policy Acknowledgment affirming their agreement to follow Terra Dotta's confidentiality and security standards for handling sensitive information.

In accordance with the **Terra Dotta Security Awareness Policy** the Company conducts annual training and review of information security procedures with all staff. Employees who handle sensitive information receive ongoing training on the importance of confidentiality of sensitive information. Employees are trained in the proper use of computer information and passwords. Training includes controls and procedures to prevent employees from providing sensitive information to unauthorized individuals and on how to properly dispose of sensitive information.

Terra Dotta conducts background checks and other forms of confirmation as needed in the hiring process for all new employees, through services provided by ADP.

Once an employee concludes his/her employment, either voluntarily or involuntarily, such employee's access to sensitive information is promptly terminated.

Reference: PCI DSS v3.2 requirement 12.6 (12.6.1 – 12.6.2), 12.7

Secure Development

Terra Dotta's Development Team, which includes all analysts, engineers, developers, and testers, will follow the **Secure Software Development Life Cycle Policy** (or SDLC), which outlines a multifaceted program of controls, training and monitoring for to ensure quality, security and continuous improvement. The SDLC uses OWASP resources as the basis of its practices and training.
Reference: PCI DSS v3.2 requirement 6.3

Acceptable Computer and Network Use Policy

This acceptable use policy governs the use of Terra Dotta computers and networks. Users of these resources are responsible for complying with this policy. All existing laws (federal and state) and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct. Client institutions operating computing and network facilities that are reachable via the Terra Dotta network may have their own policies governing the use of those resources. When accessing remote resources from Terra Dotta facilities, Company users are responsible for obeying both the policies set forth in this document and the policies of the client institutions.

Terra Dotta users are granted use privileges to access Company systems. These privileges are accepted with the condition that system administrators have the right to access user files when necessary to protect the integrity of computer systems or the rights or property of the Company and the Company's clients. For example, system administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information which may be used as evidence in a court of law.

Conduct which violates this policy includes, but is not limited to the activities in the following list.

- Unauthorized use of a computer account.
- Using the Company Network to gain unauthorized access to any computer systems.
- Knowingly or carelessly performing an act that will interfere with the normal operation of computers or networks.
- Knowingly or carelessly running or installing malware on any computer system or network, or giving malware to another user.
- Removing or disabling anti-malware or other security software, leaving computer systems vulnerable.
- Violating terms of applicable software licensing agreements or copyright laws.
- Violating copyright laws through inappropriate reproduction or dissemination of text, images, etc.
- Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mails.
- Initiating or propagating electronic chain letters.
- Inappropriate mass mailing.
- Forging the identity of a user or machine in an electronic communication.
- Accessing or transmitting pornographic material.
- Transmitting or reproducing materials that are slanderous or defamatory.

- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

Data Transmission, Handling and Retention

Terra Dotta must ensure that all electronic sensitive information is encrypted in transit. Terra Dotta will instruct clients to always transmit electronic sensitive information to Terra Dotta via secure, encrypted methods. If sensitive data must be sent over an open, public network (i.e., the Internet), strong cryptography such as TLS, SSH, or IPSEC must be used to encrypt the data. If a wireless network is used to transmit sensitive data, strong encryption (i.e. WPA2, IPSEC or TLS) must be used.

All hosted production websites are to be protected by TLS in user-authentication areas for data encryption of transacted information over HTTPS, either using Terra Dotta certificates or certificates provided by the customer.

Transfer of data files to and from Terra Dotta servers must be done via SSH using SFTP or SCP, an industry-standard, secure protocol for file transfer. Uploaded data files are accessed, processed and then deleted from the account-restricted SSH receiving folders. Terra Dotta’s recommended, preferred method for authentication is by shared key exchange, which must be provided to Terra Dotta from the client software.

The determination of data as sensitive will be done by following the **Data Classification Policy.** All information assets maintained by Terra Dotta must be assessed for their sensitivity in order to determine the specific handling procedures to follow, which is articulated in the **Data Handling Policy**. Each class of data will receive a classification, so that no ambiguity will exist about its proper handling.

Data security is also affected by its retention, for which Terra Dotta will follow the **Data Retention Policy** and maintain records for all data assets with specific retention requirements.

Reference: PCI DSS v3.2 requirements 3.1, 7

Service Provider Oversight

For all service engagements involving access or connections into Terra Dotta's sensitive data environments, Terra Dotta will review and monitor service providers' information security compliance programs and measures used by the service provider to protect sensitive information. Service providers that maintain compliance with PCI DSS will be trusted with regard to all controls guaranteed by their Attestation of Compliance (AoC) and associated scope documentation, wherever applicable.

In cases where PCI standards are not assured by an AoC, all service providers having access to sensitive information related to Terra Dotta will have provisions in their contracts or equivalent agreements requiring that they follow Terra Dotta's prescribed practices to safeguard sensitive information and to assure that such sensitive information is used only for the purposes set forth in the contract.

For any service providers accessing Terra Dotta's sensitive data environments, Terra Dotta will:

- Maintain of a list of those service providers.
- Obtain written acknowledgement from each service provider that they are responsible for the security of the sensitive data the service provider possesses or has access to.
- Follow an established procedure for engaging service providers that includes proper due diligence prior to engagement.
- Monitor service providers' PCI DSS compliance where applicable to Terra Dotta's own compliance.

Reference: PCI DSS v3.2 requirement 12.8 (12.8.1 – 12.8.4)

Risk Assessment

Terra Dotta must regularly identify, define, and prioritize risks to the confidentiality, integrity, and availability of its information systems, network resources and data. Terra Dotta must conduct an annual, formal, documented risk assessment of its information systems, data and network resources. The assessment must identify and prioritize the threats and vulnerabilities to Terra Dotta's information systems, data and network resources and define the likelihood and impact of risks.

The report must identify the significant risks to Terra Dotta information systems, data and network resources that have been identified during the past year, the risks that have been accepted and which risks have been mitigated.

The **Risk Assessment Policy** is maintained separately to specify the process in further detail.
Reference: PCI DSS v3.2 requirement 12.2

Incident Response

Whenever there is suspicion of an incident affecting the availability, integrity or security of sensitive data, Terra Dotta employees and others governed by this policy must consult the **Incident Response Policy** to determine whether to implement the **Incident Response Plan** (IRP), which is details the time-sensitive actions to be taken in such events. In many cases, Terra Dotta has a contractual obligation to its clients to follow such procedures and provide timely notifications. Terra Dotta will apply the most demanding requirements, per all of its client contracts, to ensure compliance.

Terra Dotta maintains multiple systems and procedures to prevent, detect, and respond to attacks, intrusions, and system failures. The ISOs regularly review network access and security policies and procedures, as well as protocols for responding to network attacks and intrusions.
References: PCI DSS v3.2, requirement 12.10

Business Continuity Management

The objective of business continuity management is to counteract interruptions to business activities, protect critical business processes from the effects of failures of information systems, and ensure timely resumption after interruption. As such, Terra Dotta shall ensure that redundant systems, where appropriate, are in place to support operations. Terra Dotta will maintain on-site and off-site backups to protect against system failures and major disasters. In the event of a disaster resulting in unrecoverable loss of a data center facility, services will be restored at one of our hosting providers' alternate locations. Complete disaster-recovery procedures are currently in development.

Evaluation and Revision of the Information Security Policy

This policy is subject to periodic review and adjustment. Adjustments might be necessary or advisable due to changes in technology, changes in laws, and the assessment of internal or external threats to the security and integrity of the sensitive information, among other reasons. Continued administration of the development, implementation and maintenance of this and the related security policies will be the responsibility of the CTO, who may delegate specific responsibility for implementation and administration as appropriate.

Related Security Policies

As part and parcel of this master Information Security Policy, Terra Dotta maintains additional policy and procedural documentation, as summarized and linked below. Adherence to the Information Security Policy (this document) explicitly includes adherence to all policy documents and procedures referenced here.

Firewall Configuration and Management Policy

The protection of Terra Dotta's sensitive data environments is dependent on network security devices (firewalls) that gate the destinations, origins and types of traffic permitted. This control is implemented through established policies in the firewall devices that serve to segment networks from one another as necessary for general security and for compliance with PCI standards. The policy and procedures for firewalls must be maintained and reviewed regularly as one of the most critical aspects of systems security.

Secure Configuration Policy

This policy is to ensure the servers in Terra Dotta's sensitive data environments are configured and maintained according to industry and vendor standards of security.
Reference: PCI DSS v3.2 requirement 2.2

File Integrity Policy

File integrity monitoring must be performed to ensure that no modifications have been made to content files, operating system critical files, executables, configuration files, and audit logs for systems and applications transmitting, processing, and/or storing sensitive data.
Reference: PCI DSS v3.2 requirement 10.5.5

Time Synchronization Policy

Server and network appliance time synchronization is critical to proper functionality of systems.
Reference: PCI DSS v3.2 requirement 10.4.

Anti-malware Policy

Terra Dotta will use our data centers' managed service for anti-malware to ensure protection of all our servers according to the requirements of this policy.
Reference: PCI DSS v3.2 requirement 5

Testing and Scanning Policy

Terra Dotta maintains a team of dedicated QA specialists for regular and ongoing testing of Terra Dotta software, targeting stability, security, usability, performance and data integrity. Additionally, Terra Dotta employs a variety of services and procedures for PCI standards-compliant scanning of our application and sensitive data environments, as specified in the linked policy.
Reference: PCI DSS v3.2 requirement 11.2

Log Management Policy

Along with IDS and regular scans for vulnerabilities, a thorough monitoring plan includes centralized log management and review. Terra Dotta will use the MSS provided through NTirety and will monitor the service under the terms of this policy. File Integrity Monitoring will be maintained through operating system components, with FIM logs also pushed to the logging MSS.
Reference: PCI DSS v3.2 requirement 10 (except 10.4)

Change Management Policy

All changes to sensitive data environments must be requested and authorized using a Change Request Form, following the terms of this policy.
Reference: PCI DSS v3.2 requirement 6.4.5

Access Management Policy

Terra Dotta will ensure that access to sensitive information is limited to those individuals who have a business reason for having access to such information. Every individual with access to sensitive data systems is assigned a separate username and password and is required to affirm that they will adhere to all relevant Terra Dotta security policies.
Reference: PCI DSS v3.2 requirement 8

Password Management Policy

The following guidelines of this policy are to ensure secure and consistent practices in password management. While individual applications will screen for most of these guidelines as an aid in creating secure passwords, the employee has primary responsibility for creating and securing a good password.
References: PCI DSS v3.2, requirements 2.1, 8.2, 8.4

Controls and Dependencies Specific to PCI DSS

Terra Dotta's use of the PCI DSS as a framework for our security practices is both **general**, to strengthen our operations in all aspects of security, and **specific** to our obligation to provide certified secure operations as a service provider to our clients who wish to link to payment gateways from their Terra Dotta Software website. In our current operational setting, we have determined to limit the scope of our PCI certification to the software hosting service we provide through our US-based (Louisville, KY) data center managed by NTirety, Inc. We will not provide service for payment gateway integrations in any other hosting environment (i.e., neither in our Melbourne, Australia, data center nor at remote installations at client facilities). Any existing client payment gateway integrations at remote installations outside of the NTirety Louisville data center are outside the scope of our current compliance certification. This policy may be changed in the future should we decide to expand our provided services. By taking this approach, we are able to better focus our efforts and achieve compliance in the timeframe demanded by our current and prospective clients.

Remote Access, Jump Server and Multi-factor Authentication

As the most effective and immediate means of network segmentation. Terra Dotta will secure remote access to the CDE, Terra Dotta will maintain its firewall and Windows domain in such a way as to restrict all administrative access to a single point of entry in the network: a Jump Server, highly secured, which acts as nothing more than a terminal from which other connections can be made for system administration.

Remote access into the Jump Server consists of the following steps:

- VPN Login: Each individual who needs to access the CDE for administrative purposes must have an individual VPN user account. VPN logins, as all others, are subject to the Access Management Policy and must be kept in sync with related user accounts. Critical to the implementation of Jump Server network segmentation is that firewall policies be maintained that only provide VPN dialup users access to the Jump Server and no other networked devices.
- Local User Account: The Jump Server shall not be a member of the Windows domain with the CDE networked devices. Every individual accessing the CDE must have an individual local user account on Jump Server, with all access logged. Local Jump Server user account will be managed following the Access Management Policy.
- MFA: Access to the Jump Server must require multi-factor authentication. This means that there is authentication with something the user knows (password, passphrase) and something the user has (mobile phone SMS/app, key fob, fingerprint, individual certificate). MFA devices and app user accounts must be managed following Access Management Policy (i.e., revoked at time of termination of access change).

Remote access must be over a secure, encrypted connection or over a dedicated private line, and logged. Remote access may not be used unless for business purposes, and all users must be approved by Terra Dotta ISOs prior to being granted this access following the Access Management Policy. Only Terra Dotta-approved remote access technologies may be used. Idle RDP sessions will automatically disconnect after 60 minutes and the user will be required to re-authenticate.

Reliance on NTirety PCI-Compliant Services

The "cardholder data environment" (CDE) in traditional PCI terms refers to environments that store, process or transmit cardholder data. In practice and in accordance with this policy and our SDLC, **Terra Dotta never stores, processes or transmit cardholder data.** However, in version 3.0 of the PCI DSS, the scope definition has shifted in a critical way, such that

> *"Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or* ***may impact the security of (for example, name resolution or web redirection servers) the CDE."***
>
> (from PCI DSS v3.2, p. 10, under "Scope of PCI DSS Requirements").

On the advice of several Qualified Security Assessor (QSA) companies, as well as the dictates of some of our clients' security compliance officers, we are led to interpret this change as including Terra Dotta's Payment Gateway Integration service offering to be within the scope of PCI DSS.

Since Terra Dotta (a) does limit its PCI scope by keeping cardholder data out of our network entirely and (b) utilizes services provided by a PCI-compliant hosting provider, and also because (c) NTirety provides all controls over the physical infrastructure security and network components, many of the required controls of the DSS are either assessed as **Not Applicable** to our operations (e.g, Section 3, which deals with stored cardholder data), or **In Place** through the use of NTirety's certified compliant services. We depend on NTirety's continuous compliance status for the foundation of our own certification, and as such, we must monitor their compliance annually.

In addition to the physical infrastructure and network security provided by NTirety, the specific PCI-compliant optional services that Terra Dotta obtains from NTirety are as follows:

PCI DSS Req	**Service**	**Product or Service**
5	Anti-malware Service	Symantec Endpoint Protection
10 (most of)	Log Management and Review	Alert Logic Log Manager with Log Review
10.4	Time Synchronization (NTP)	N/A (NTirety servers w/ registry settings)
11.2	Vulnerability Scans (internal & external weekly; ASV external quarterly)	Alert Logic Threat Manager
11.4	Intrusion Detection Service (IDS)	Alert Logic Threat Manager with Threat Watch