THREATMATE™
INQUISITIVE SECURITY

Data Protection Policy Global

PURPOSE

The Company recognizes how important Data Protection is to our Company as a whole, our Employees, and our Customers.   The policy provides guidelines:

- To establish consistent and uniform guidelines for managing various categories of information;
- To define employee and management responsibility for safeguarding information;
- To define procedures regarding safeguarding information;
- To comply with internal controls rules and requirements, and to ensure the proper handling of information within our organization.

SCOPE

This policy applies to ThreatMate, Inc. (the "Company") and its subsidiaries and to all of the Company's employees, consultants, and contractors.

RESPONSIBILITY

The Company's Administrative department is responsible for the development and maintenance of this policy. The Administrative department shall audit for proper set up and internal controls on a periodic basis. Any exceptions to this policy must be approved in writing and in advance by either the CFO or the CEO.

It is each employee's responsibility to ensure compliance with this Policy.

POLICY

This Data Protection Policy provides a high level view of the Company's policy. The Policy is intended to establish a framework for managing risk and protecting the Company's data. The establishment of this policy outlines the Company's commitment to information security, including identification of potential risks, development of protocols to mitigate risk, and enforcement of policies.

It is the Company's policy to treat Data and its protection as an important aspect of our business process.
We categorize data into three classifications:
Public
Internal
Confidential/Restricted

Public information is defined as information that is open to the general public. It is information with no existing local, national, or internal legal restrictions on access or usage. It is information that is available to all employees and all individuals or entities external to the corporation.
Examples include:
Publicly posted press releases, publicly posted marketing material
Publicly posted job announcements.

Internal information is defined as information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or thither use. This classification applies even though there may not be a legal requirement. Internal Data is information that is restricted to personnel who have a legitimate reason to access it .

Examples include:
General employee data (excludes SSN, salary)
Contracts, customer lists, price lists, customer trouble tickets, customer information
Engineering Source Code

Confidential/Restricted is defined as highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization is required for access because of legal, contractual, privacy or other constraints. Confidential data has a high level of sensitivity.

Examples include:
Employee SSN, Salary, Passport information
Customer data provided as part of a trouble ticket
Customer data provided as part of migration or set up
Customer data collected using our software
Credit card information related to payment processing

THREATMATE™
INQUISITIVE SECURITY

Data Protection Policy - Customer Data

PURPOSE

The Company recognizes how important Data Protection is to our Customers and their specific data. The policy provides guidelines:

- To establish consistent and uniform guidelines for managing various categories of information;
- To define employee and management responsibility for safeguarding information;
- To define procedures regarding safeguarding information;
- To comply with internal controls rules and requirements, and to ensure the proper handling of information within our organization.

SCOPE

This policy applies to ThreatMate, Inc. (the "Company") and its subsidiaries and to all of the Company's employees, consultants, and contractors.

RESPONSIBILITY

The Company's Administrative department is responsible for the development and maintenance of this policy. The Administrative department shall audit for proper set up and internal controls on a periodic basis. Any exceptions to this policy must be approved in writing and in advance by either the CFO or the CEO.

It is each employee's responsibility to ensure compliance with this Policy specifically as it relates to customer data and its retention and use.

This portion of the Data Protection Policy relates to customer data and its retention and use.

COLLECTION

What data is collected: As part of our Software, we collect and maintain customer data at a meta level. Detailed customer information, i.e. passwords, credit card numbers, is not gathered or maintained by our Software. The information we obtain varies depending on the product you are using.

Adversary View: The data obtained through this product includes network information, connected devices on the network, device open ports and company email addresses. The company information is encrypted in transit using HTTPS authenticated encryption and sent to a dedicated and segmented cloud database which is managed and hosted on Google Cloud Platform. Access to this data is strictly guarded by the use of access controls. Every customer is assigned an individual account that is not commingled with other customer data. The account is password protected and accessed only by the development team on a need to know basis. Additionally, a customer can manage the access to this data by using a 3 level access control system that is built into the product dashboard. It provides 3 account access levels: standard account, admin account and super admin account.

When customer information is used in the aggregate, across multiple customers, it is fully anonymized. This is done by stripping all references to the customer or its location, all references to internal IP addresses and device hostnames and all references to customer email addresses.

Defender View: The data obtained through this product includes device operating system, hardware information such as the motherboard vendor, model and serial number, number of CPUs, firmware version, running processes, installed applications, local and remote network connections, existing users and groups, login history and other operating system information. The collected information is encrypted in transit using HTTPS authenticated encryption and sent to a dedicated and segmented cloud database which is managed and hosted on Google Cloud Platform. Access to this data is strictly guarded by the use of access controls. Every customer is assigned an individual account that is not commingled with other customer data. The account is password protected and accessed only by the development team on a need to know basis. Additionally, a customer can manage the access to this data by using a 3 level access control system that is built into the product dashboard. It provides 3 account access levels: standard account, admin account and super admin account.

RETENTION

How long is data retained: Data is retained at a customer level for a maximum of 7 years but not less than 1 year. Customer data may be retained but is not required to be retained should the customer terminate its contract with us. If required by regulatory compliance, data can be deleted upon receipt of written request to legal@threatmate.com.

ACCESS

Data is available on a limited access basis via our Google Cloud Platform account. Engineering, Customer Service, and Business Analytics and Reporting teams currently have access to the information on a need to know basis. Access is password protected audit logged. Review of access to the Google Cloud Platform is performed by our executive team once per quarter to ensure only necessary employees have access. Procedures are maintained by our executive team to ensure access is appropriately terminated when applicable (eg end of employment.)

Customer data is used for threat detection services, dashboard reporting, email alerting, in software reporting, product development.

Anonymized customer data is used for global insight reporting and other cross-customer reporting and analysis.