MORLEY

THIRD PARTY DATA PRIVACY & SECURITY TRAINING

By doing business with Morley, you agree to take necessary precautions to protect data belonging to Morley and our clients. It is critical that you take this responsibility seriously. We may be entrusting you with confidential and legally protected information, including the names of program participants.

Morley is relying on you to take all measures to keep data secure. However, in the unfortunate event that a data breach occurs, **you must inform Morley IMMEDIATELY**.

Your minimum responsibilities are listed below. Morley has the right to audit your systems and security measures at any time. If you have any questions about your obligations, contact Morley at *compliance@morleynet.com* and copy *security.administrator@morleynet.com*.

VENDOR RESPONSIBILITIES – DATA PROTECTION

Vendor shall protect and secure personally identifiable information (PII) through administrative, physical, and other measures to implement privacy or data protection policies and procedures currently in place. Taking into account the risks presented by the use of PII, Vendor will implement and maintain reasonable and appropriate practices, procedures, and systems, including administrative, technical, and physical safeguards to:

› Protect the security, confidentiality, and integrity of PII;
› Ensure against anticipated threats or hazards to the security or integrity of PII;
› Protect against unauthorized access to or use of PII

These measures shall include as appropriate:

› Measures to ensure that only authorized personnel can access PII
› An appropriate level of security, taking into account all risks presented by processing PII (e.g., accidental or unlawful destruction, loss or alteration, and unauthorized or unlawful storage, processing, access, or disclosure)
› Pseudonymization and encryption of PII
› Systems protections (e.g., intrusion, data storage, and data transmission protection)
› Physical security measures
› Information access controls and restricted disclosures
› A written data security plan and employee training
› A process for regularly testing and evaluating the effectiveness of PII security measures and to identify vulnerabilities in systems used to provide these processing services to Morley
› Ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems
› Ability to restore access to personal data in a timely manner in the event of an incident
› When processing European PII, Vendor agrees to take measures required by Article 32 of the GDPR

VENDOR RESPONSIBILITIES – DISCLOSURE OF PII

In addition to the use and protection requirements described above, Vendor's disclosure of PII is also subject to the following requirements:

Vendor personnel: Vendor shall not disclose PII to its personnel or allow its personnel to access PII except in the following instances:

› Vendor personnel require PII to provide the services
› With prior written approval of Morley
› As required by applicable laws

When permitted, disclosure or access to PII shall be limited to the specific information necessary to complete the task. Vendor shall inform personnel with access to PII of the confidentiality requirements and train these personnel on the proper use and protection of PII.

Third Parties: Vendor shall not sell, disclose, provide, or exchange PII to any third party other than Vendor's service providers and only upon the express written permission of Morley. Vendor may disclose PII to a service provider when required for Vendor to obtain products or services necessary to complete its obligations, subject to Morley's written consent. When permitted, disclosure of or access to PII shall be limited to the specific information needed for the service provider to complete its assigned task.

Vendor will ensure that the third party signs a written agreement with Vendor to assume obligations at least as stringent as Vendor's obligations to Morley, including but not limited to:

- Restricting its use of PII to the use specified in the agreement between Vendor and the third party (which use must further and be limited to Vendor's performance under its obligations)
- Complying with all applicable laws and Morley's privacy policies
- Providing notice of any actual or reasonably suspected security breach, unauthorized access, misappropriation, or other compromise of the security, confidentiality, or integrity of Morley PII

Vendor is responsible for the acts or omissions of its personnel and any third party to whom it transfers or provides access to PII, and shall refer any person seeking access to any PII to Morley.

NOTICE OF BREACH OF PII

Since no two incidents will be the same, this incident response procedure is meant to provide the computer incident response team with the framework to handle an incident. They will have to quickly analyze each specific incident, with the goal to limit the damage, maintain the security of other systems and/or applications, contact the appropriate people and document the incident. They must also control the release of information about the incident, both within the company and to external sources, to control uncertainty, fear, and any disturbance the company might otherwise suffer. Any reported incident warrants investigation, and an initial assessment may require immediate containment.

If the incident is an intrusion or attack involving security measures being breached or customer information being compromised, the company's policy is to deny current and future access to the attacker to contain the situation. This short-term containment stops an intruder's access to the compromised system(s), limits the extent of the intrusion, and prevents an intruder from causing further damage. Examples of containment include disconnecting the external border router to the internet, disabling a User ID, or disconnecting a server from the network. Vendor must decide on the best method to deny access based on the circumstances.

Other types of incidents will require Vendor to determine if containment, remediation, or some other action is necessary, based on the circumstances. It is important to remember that any changes to the compromised system(s), including containment, may destroy information required to assess the cause of an intrusion. Vendor needs to exercise caution during the containment phase to ensure the steps taken will also preserve as much information and evidence as possible for future investigation.

Vendor will notify Morley immediately, within 24 hours of discovering or otherwise receiving information of an actual or reasonably suspected security breach, unauthorized access, misappropriation, or other compromise of the security, confidentiality, or integrity of PII, including notice of a security breach from Vendor's permitted service provider. Where applicable, Vendor must act immediately to prevent any further breach and notify Morley at *compliance@morleynet.com*, with a copy to *security.administrator@morleynet.com*. In the event of a security breach, Vendor shall implement the remediation plan agreed to by the Parties.