MASTER WiZR

Data Breach Notification Policy

1.0 Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

MASTER WiZR Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how MASTER WiZR's established culture of openness, trust and integrity should respond to such activity. MASTER WiZR Information Security is committed to protecting MASTER WiZR's contractors, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.1 Background

This policy mandates that any individual who suspects that a theft, breach or exposure of MASTER WiZR Protected data MASTER WiZR Sensitive data has occurred must immediately provide a description of what occurred via e-mail. This Information Security Administrator will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

2.0 Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of MASTER WiZRmembers. Any agreements with vendors will contain language similar that protects the fund.

When working with remote employees, contractors, or third-party vendors, it is essential to ensure that the handling and storage of data remain secure. This section provides specific guidance for these individuals to ensure that they understand their responsibilities regarding data security.

Remote employees, contractors, or third-party vendors must follow the same data handling and storage practices as on-site contractors. All data should be handled with care, and measures should be taken to prevent data breaches or loss. The following guidelines should be followed:

- Access to data should be limited to individuals who require it to complete their job duties.
- Passwords should be strong, unique, and changed regularly.
- Devices used to access company data should be secured with up-to-date antivirus software and firewalls.
- Data should be encrypted both in transit and at rest.
- Cloud-based storage solutions should be used only if approved by the company, and should meet the company's security standards.
- Data should not be downloaded onto personal devices or sent to personal email addresses.
- Any suspicious activity should be reported to the company's IT department immediately.
- It is important to understand that the responsibility for data security rests with everyone who handles company data, including remote employees, contractors, and third-party vendors. Failure to follow these guidelines may result in disciplinary action, up to and including termination of the contract or employment agreement.

By following these guidelines, remote employees, contractors, and third-party vendors can help ensure the security of company data and protect the company's reputation.

To ensure the security of company data, it is important to establish protocols for the use of personal devices and networks by remote employees, contractors, or third-party vendors. The policy should require the use of secure virtual private networks (VPNs) and two-factor authentication to access company data from personal devices or networks.

Employees, contractors, or third-party vendors should be informed of the importance of using secure devices and networks to prevent unauthorized access or data breaches. The policy should also provide specific guidance on how to set up and use secure VPNs and two-factor authentication.

In addition, the policy should outline procedures for reporting lost or stolen devices and for revoking access to company data in case of termination of employment or contract. By establishing clear protocols and guidelines for the use of personal devices and networks, the company can ensure the security of its data and protect against potential security threats.

3.0 Policy Confirmed theft, data breach or exposure of MASTER WiZR

3.1 Identification and Containment

Upon identification of a theft, data breach, or exposure containing MASTER WiZR Protected data or MASTER WiZR Sensitive data, immediate action will be taken to contain the incident and remove all access to the affected resource. The incident will be reported to the Executive Director, who will chair an incident response team to handle the breach or exposure.

3.2 Incident Response Team

The incident response team will consist of members from various departments, including IT Infrastructure, IT Applications, Finance, Legal, Communications, Member Services (if Member data is affected), Human Resources, the affected unit or department that uses the involved system or output, or whose data may have been breached or exposed, and additional departments or individuals as deemed necessary by the Executive Director.

3.3 Assessment and Investigation

The incident response team will assess the scope of the breach or exposure and investigate the cause and extent of the incident. The team will also determine the impact of the breach or exposure on MASTER WiZR, its clients, and partners.

3.4 Notification and Communication

If necessary, MASTER WiZR will notify its clients and partners, as well as relevant regulatory authorities and law enforcement agencies, of the breach or exposure. The team will also develop a communication plan to keep employees, contractors, clients, partners, and the public informed about the incident.

3.5 Mitigation and Recovery

The incident response team will take immediate steps to mitigate the impact of the breach or exposure and prevent any further damage. The team will also develop a recovery plan to restore MASTER WiZR's systems, data, and services to normal operations.

3.6 Lessons Learned and Improvement

After the incident has been contained and resolved, the incident response team will conduct a post-mortem analysis to identify lessons learned and areas for improvement. The team will also update policies, procedures, and controls to prevent similar incidents from occurring in the future.

3.7 Employee/Contractors Responsibilities

All contractors have a responsibility to report any suspected or confirmed theft, data breach, or exposure of MASTER WiZR Protected data or MASTER WiZR Sensitive data. Contractors must also cooperate fully with the incident response team during an investigation and adhere to all policies, procedures, and controls related to data security and incident response. Failure to comply with these policies may result in disciplinary action, up to and including termination.

The incident response team will follow a predefined process to ensure that the breach or exposure is contained, the extent of the damage is determined, and appropriate action is taken to mitigate any potential harm to MASTER WiZR, its clients, or its stakeholders.

The process includes the following steps:

- Isolation of the affected resource to prevent further damage or exposure
- Analysis of the affected resource to determine the extent of the damage or exposure
- Notification of relevant internal and external parties, including affected employees, contractors, clients, and authorities if necessary
- Implementation of remedial measures, such as the restoration of affected systems or networks and the enhancement of security measures to prevent future incidents
- Evaluation of the incident to identify any lessons learned and to update MASTER WiZR's security policies and procedures accordingly

The incident response team will work diligently and effectively to ensure that all necessary steps are taken to safeguard MASTER WiZR's data and minimize the potential impact of any breach or exposure. MASTER WiZR recognizes the critical importance of data security and is committed to maintaining the highest standards of protection for all sensitive information.

Confirmed theft, breach or exposure of MASTER WiZR data

When a confirmed theft, breach or exposure of MASTER WiZR data occurs, the following steps will be taken:

- The Executive Director will be notified immediately by the IT department or the designated security officer.

- The IT department, along with the designated forensic team, will analyze the breach or exposure to determine the root cause and scope of the incident. This will include identifying the type of data involved, the source of the breach or exposure, and any potential impact on individuals or the company as a whole.

- The incident response team, chaired by the Executive Director, will be activated to handle the breach or exposure. The team will include members from IT infrastructure, IT applications, finance (if applicable), legal, communications, member services (if member data is affected), human resources, the affected unit or department that uses the involved system or output, and additional departments based on the data type involved or as deemed necessary by the Executive Director.

- The incident response team will develop a plan of action to contain the breach or exposure, mitigate the damage, and restore systems and data to their pre-incident state. The plan will also include steps to notify affected individuals or entities, as required by law or regulation.

- The incident response team will work with external law enforcement agencies, regulatory bodies, and other stakeholders as necessary to investigate the breach or exposure and provide any necessary information.

- The incident response team will conduct a post-incident review to identify lessons learned and make recommendations for improving the company's security posture and incident response procedures.

- The Executive Director will be responsible for communicating the details of the breach or exposure to senior management, the Board of Directors, and other stakeholders, as necessary.

Overall, the company takes the security of its data seriously and is committed to taking swift and appropriate action in the event of a confirmed theft, breach or exposure of MASTER WiZRy data.

Develop a communication plan.

Work with MASTER WiZR communications, legal and human resource departments to decide how to communicate the breach to: a) internal staff, b) the public, and c) those directly affected.

3.2 Ownership and Responsibilities

Roles & Responsibilities:

- Sponsors - Sponsors are those members of the MASTER WiZR community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any MASTER WiZR Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Information Security Administrator is that member of the MASTER WiZR community, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the MASTER WiZR community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary contractors and volunteers.
- The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

4.0 Enforcement

Any MASTER WiZR personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

5.0 Definitions

Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;

Plain text – Unencrypted data.

Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

Protected Health Information (PHI) - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered.

Protected data - See PII and PHI

Information Resource - The data and information assets of an organization, department or unit.

Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

Sensitive data - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.