American Water Works Association
MinnesotaSection

Information Security Policy

Contents

Introduction

Definitions

Media – documents, files, or data, both on paper and electronic.
Assets – Minnesota Section American Water Works (MNAWWA) owned computers, servers, storage devices, applications, websites, or anything else that can store media.
User – A person operating or handling MNAWWA owned assets or media.
Service Provider – Any other company that has access to cardholder information or has influence over the security measures to keep that information safe.

Scope

This policy applies to MNAWWA volunteers, employees, third-parties, service providers, contractors, and temporary employees.

This policy applies to all systems, applications, and electronic equipment owned, borrowed, or leased by MNAWWA and all MNAWWA locations where cardholder data is present.

Distribution

This policy is to be distributed to all MNAWWA volunteers, employees, contractors, and service providers. Also, this policy is to be distributed to any third party that is granted access to MNAWWA assets or media.

Responsibilities

Users are required to:

- Follow MNAWWA policies at all times.
- Acknowledge their agreement with this Information Security Policy before first accessing MNAWWA's assets or media.
- Safeguard MNAWWA's assets and media per the policies within this Information Security Policy.
- Report any deviation from this Information Security Policy to the executive board immediately.

IT Committee is required to:

- Implement and maintain security controls for electronic assets.

Secretary/Treasurer is required to:

- Monitor and control access, transmission, storage, and destruction of media.
- Monitor PCI compliance status of service providers.
- Review and update this Information Security Policy.

Executive Board is required to:

- Take ultimate responsibility for information security management and for safeguarding MNAWWA's assets and media.
- Respond to reported deviations from this Information Security Policy.
- Approve updates or changes to this Information Security Policy.

Review Schedule

This policy is to be reviewed and updated annually by the Secretary/Treasurer and approved by the Executive Board.

Anti-Virus Software

Deployment

Anti-virus software must be deployed on all MNAWWA owned or leased servers, computers, and gateways which are considered to be those commonly affected by viruses. The anti-virus software should be an up to date/current enough version that it protects against spyware and adware.

Configuration

Configuration of the software must follow the vendor-provided guidance and standards, with exceptions reviewed and approved by the IT Committee. The software should be configured so that users cannot disable or tamper with it. Automatic updating should be enabled.

Scanning

Anti-virus software should be set to scan in “auto-protect” mode to automatically scan new files in creation, incoming and outgoing email attachments, and downloaded files. A full computer scan should be set to be performed at least weekly.

Logging

Anti-virus event logs are to be generated and retained for at least 365 days. These logs should contain dates of scans performed and incidents found.

Responsibilities

The IT Committee is responsible for training users on how to prevent, detect, and respond to an incident which may be related to a virus. Specifically, users should know not to click on an attachment from an unknown person and how to identify if their system is running slow or acting up. Users are to report suspected incidents to the IT Committee.

Media Classification

Classification

Any media which contains cardholder information or other sensitive information should be labeled as "<Confidential>". Other sensitive information includes social security numbers and login information to sensitive online accounts.

Handling

Once the media has been classified, it is to be transmitted, processed, used, and/or stored following the methods outlined in the Media Handling Policy.

Incident Response

Should <Confidential> media be intentionally or unintentionally accessed, viewed, or used by an unauthorized party, the executive board must be notified and respond to the incident.

Requests for Access to Confidential Media

The Secretary/Treasurer is ultimately responsible for individuals and applications that have access to MNAWWA media, and is to review the access permissions to confidential media on an annual basis.

Awareness

MNAWWA volunteers are to be trained and made aware of the media classification and handling requirements. Those who have business requirements to view, access, and use <Confidential> media are to receive specialized training on how to properly handle such items.

Media Handling

Cardholder Data

Cardholder data may never be transmitted electronically using any end-user methodologies, such as e-mail, unless specifically approved by the Secretary/Treasurer for a valid business need. If required to transmit cardholder data, it must be in unreadable format (for example, encrypted, masked, truncated). Users may also not store cardholder data without specific approval to do so from the Secretary/Treasurer at which point it must also be retained in a protected format.

Handling Requirements for Media Labeled as <Confidential>:

Access:	Business need-to-know only. Must be approved by Secretary/Treasurer.
Non-Disclosure (NDA):	MNAWWA third-parties, contractors, and volunteers may only access this media after signing a NDA.
Email:	Only individuals approved by the Secretary/Treasurer to transmit this media by email may do so, and then only if the email and its attachments are approved using a MNAWWA-approved encryption method. A receipt request should be used or requested.
Internet:	This media may never be posted/communicated via the internet. This includes posting to websites or using internet messaging technologies.
Fax:	The person sending the fax with this media is required to be present at the fax machine to verify that it has been sent and is not stored in the memory. A receipt request should be used or requested.
External Mail:	This type of media is to be packaged in a secure manner and delivered by a commercial delivery service which can be tracked. A return receipt should be used or requested, such as a delivery signature. The Secretary/Treasurer must be notified prior to mailing.
Printing:	This type of media should not be printed unless absolutely needed for business purposes, and after approval from the Secretary/Treasurer. If a printer saves an electronic file of the printed media, the electronic file must be permanently erased immediately after printing.
Print Storage:	Printed media of this type is required to be within eyesight or within possession at all times, or locked up in a secure manner or location.
Electronic Storage:	Stored media of this type may not be retained in a readable electronic format and is to be truncated, masked, or encrypted using a MNAWWA-approved method. This includes media storage on computers, servers, backup tapes, etc.
Logs:	The Secretary/Treasurer must maintain a list of all individuals that have been granted access to this type of media. Also, the Secretary/Treasurer must log all changes of physical location for this type of media.

Media Retention

Retention of Cardholder Data

Cardholder data should only be retained for the minimum length of time needed for processing.

Retention of Sensitive Authentication Data

Sensitive Authentication Data (the magnetic strip, PIN blocks, CVV) may never be stored after authorization, unless there is a specific business need to retain this data. The PCI Data Security Standards have specific requirements for what comprises a business need for the retention of this data. The Sensitive Authentication data may be retained prior to authorization, but must be safeguarded following the requirements outlined for “Confidential” data in the Data Handling Policy.

Retention Periods

Cardholder data is to be destroyed when it is no longer needed for business or legal reasons. A review of media is to be conducted quarterly to determine if any cardholder data still needs to be destroyed. If cardholder data is to be retained after processing, it must be assigned and labeled with a specific retention time.

Other confidential media should be assigned specific retention times based on legal and regulatory requirements. A review of all confidential media is to be conducted annually to determine if any data still needs to be destroyed.

Responsibilities

The Secretary/Treasurer is ultimately responsible for ensuring that confidential media is not retained past the defined retention periods and for performing reviews of retained media to determine if any media needs to be destroyed.

Media Disposal

Disposal Requirements for Electronic Media Labeled as <Confidential>:

Hard drives and other electronic storage devices containing <Confidential> files are to be securely wiped using an industry-strength wiping tool or reformatted prior to being transferred to another party. If the storage device is not going to be reused, it should be physically destroyed in addition to being securely wiped. Users should be made aware of the importance of safely destroying and deleting this data.

Cardholder data must be securely erased when it is no longer needed (see *Media Retention Policy*).

Disposal Requirements for Printed Media Labeled as <Confidential>:

Printed documentation labeled as <Confidential> must be shredded using a cross-cut shredder. Anyone handling documentation with sensitive information must have such a shredder located nearby or a locked bin if a third-party is used to pick up the documentation for shredding. These documents are to be securely retained up to their destruction. Third-party vendors used to shred documentation must have provided a signed Non-Disclosure Agreement and agree to MNAWWA's terms and conditions of protecting the sensitive data. Users should be made aware of the importance of safely destroying these documents.

Cardholder data must be securely erased when it is no longer needed (see *Media Retention Policy*).

Responsibilities

The Secretary/Treasurer is ultimately responsible for ensuring that electronic and printed media is disposed of in a secure manner.

Third-Parties

Third-parties must receive a copy of MNAWWA's data labeling, handling, retention, and disposal policies and follow them. Periodic checks should be made by MNAWWA to ensure that the third-party does not violate the policies.

Service Providers

List of Service Providers

Company Name	Date of Initiation	Date of PCI Verification
Yourmembership.com	7/2014	1/12/2016
Bluepay	7/2014	1/5/2016

Engagement of Service Providers

Prior to the use of a service provider, a review and risk assessment of the service provider will be conducted by the MNAWWA executive board. This review will include verifying the service provider's PCI compliance status, reviewing security policies, collecting feedback from other users, and conducting a verbal interview with a qualified employee of the service provider.

Agreement

A written agreement must be obtained from each service provider that establishes their responsibility for the security of cardholder data that is in their possession prior to use of that service provider.

Monitoring

The PCI compliance status of each service provider listed above must be checked annually by the Secretary/Treasurer. The date of PCI verification in the above list must be updated. If a service provider is out of compliance with PCI requirements when checked, use of that service provider must be terminated.