
Aquatic Control Engineering

# Information Security Policy

Date Reviewed: 14/06/2023
Next Scheduled Review: 14/06/2024

Contents

## Introduction

This Policy document encompasses all aspects of security surrounding confidential company information and must be distributed to all Aquatic Control Engineering employees. All ACE employees must read this document in its entirety and sign the form confirming they have read and fully understand this policy. This document will be reviewed and updated on an annual basis or when relevant to include newly developed security standards into the policy and re-distributed to all employees and contractors where applicable.

## Information Security Policy

***What is Data Security?***

***Data Security is the process of securing data, whereby only authorised people can access or modify certain data. Data protection is defined as both the legal control over access to and the use of data, alongside The General Data Protection Regulation, ensuring a high level of information security is maintained.***

***GDPR is the protection of an individual's personal details when the data is collected and processed (see separate GDPR Policy.)***

Aquatic Control Engineering Limited handles sensitive cardholder information due to its business activities. Sensitive Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organisation.

Aquatic Control Engineering Limited commits to respecting the privacy of all its customers and to protecting any customer data from outside parties in line with the General Data Protection Act (See ACE GDPR Policy). ACE are committed to maintaining a secure environment in which to process cardholder information to ensure we meet these promises.

Information security incidents must be reported immediately to both the Managing Director and the GDPR representative.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

## 1. Acceptable Use; Employee code of conduct commitment

Aquatic Control Engineering company core values establish culture of openness, trust and integrity. ACE is committed to protecting all internal and external contexts of the organisation from illegal or damaging actions, either knowingly or unknowingly by individuals.

All ACE employees practice the following key areas of conduct to ensure high level of security is maintained:

- Employees must handle all company and any payment information with confidentiality and sensitivity
- Employees should take all necessary steps to **prevent** unauthorized access to confidential data which includes any payment information such as card holder data.

- Confidential data includes personnel information which should not be disclosed following GDPR steps
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use when using company equipment
- Keep passwords secure and do not share accounts. ACE authorized users are responsible for the security of their passwords and accounts
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature
- Always leave desks clear of sensitive data and lock computer screens when unattended
- You must not install unauthorised software or hardware, including modems and wireless access unless you have approval from the Managing Director
- Any suspicious behaviour will be reported immediately
- Information contained on portable computers is especially vulnerable, special care should be exercised.
- Follow the Social Media and Internet company policy

## 2. Protect Stored Data

- Sensitive or confidential data is only stored when completely necessary and for as short a period as possible.
- All sensitive cardholder data handled by Aquatic Control Engineering must be securely protected against unauthorised use at all times.

**It is strictly prohibited to store:**

1. **The contents of the payment card magnetic stripe (track data) on any media whatsoever.**
2. **The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.**
3. **The PIN or the encrypted PIN Block under any circumstance.**

## 3. Access to the Sensitive Cardholder Data

All Access to sensitive cardholder data is controlled and authorised. Any job functions that require access to cardholder data should be clearly defined in their duties.

- Any display of the card holder should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information
- No other employees should have access to this confidential data unless authorised by the Managing Director
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.

## 4. Physical Security

Access to sensitive information in media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.



T: 01777 249080
E: info@aquaticcontrol.co.uk
W: aquaticcontrol.co.uk

- Media is defined as any printed or handwritten paper, received faxes, USB, back-up tapes, computer hard drive, etc.
- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device.
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management, under no circumstances should card date be recorded without authorisation.
- Strict control is maintained over the storage and accessibility of media
- Under no circumstances do ACE store sensitive cardholder data on any computers, hard drives or servers within the business.

## 5. Protect Data in Transit

- Card holder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat or any other end user technologies.

## 6. Disposal of Stored Data

- All data must be securely disposed of when no longer required by Aquatic Control Engineering, regardless of the media or application type on which it is stored
- An automatic process must exist to permanently delete on-line data, when no longer required
- Aquatic Control Engineering will have documented procedures for the destruction of electronic media. These will require:
    - All cardholder data on electronic media must be rendered unrecoverable when deleted
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- In the unlikely case that cardholder information is written down, this should be marked as awaiting destruction and held in lockable storage container clearly marked “To Be Shredded” - access to this container must be restricted.

## 7. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness.

- Review handling procedures for sensitive information and provide training to employees
- Distribute this security policy document to all ACE employees. It is required that all employees confirm that they understand the content of this security policy document
- All employees that handle sensitive information may undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment and duties with Aquatic Control Engineering.
- Company security policies must be reviewed annually and updated in line with GDPR, ISO 9001 and current legislation

8. Credit Card (PCI) Security Incident Response Plan

Aquatic Control Engineering PCI Security Incident Response Team (PCI Response Team) is comprised of the Information Security Officer and Merchant Services. Aquatic Control Engineering PCI security incident response plan is as follows:

1. Immediately report an incident to the Information Security Officer (preferably) or to the Managing Director
2. The PCI Response Team (including any relevant third-party service provider) will investigate the incident and assist in limiting the exposure of cardholder data and in mitigating the risks associated with the incident
3. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary
4. The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred

Aquatic Control Engineering Limited PCI Security Incident Response Team is a member of the Board, Managing Director or the Information Security Officer.

**Information Security PCI Incident Response Procedures:**

A department that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform Aquatic Control Engineering Limited PCI Incident Response Team.
After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan.

**Response Plan;** In response to a systems compromise, the PCI Response Team will:

1. Ensure compromised system/s is isolated on/from the network.
2. Gather, review and analyze the logs and related information from various central and local safeguards and security controls as required
3. Conduct appropriate investigation
4. Contact internal and external departments and entities as appropriate
5. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions

All credit card companies have individual specific requirements that the Response Team must address in reporting suspected or confirmed breaches of cardholder data. These should be reviewed dependent on the case at hand.

Incident Response notifications to various card schemes

1. In the event of a suspected security breach, alert the Information Security Officer or Managing Director immediately
2. The security officer will carry out an initial investigation of the suspected security breach
3. Upon confirmation that a security breach has occurred, the security officer will alert management and begin informing all relevant parties that may be affected by the



T: 01777 249080
E: info@aquaticcontrol.co.uk
W: aquaticcontrol.co.uk

compromise

9. Transfer of Sensitive Information

- All third-party companies providing critical services to Aquatic Control Engineering Limited must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with Aquatic Control Engineering Limited's Physical Security and Access Control Compliance

10. User Access Management

- Access to Company information is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.
- Each user is identified by a unique login so that users can be linked to and made responsible for their actions.
- There is a standard level of access; other services can be accessed when specifically authorized by HR/line management.
- The job function of the user decides the level of access the employee has to data
- A request for any additional service access must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:
  Name of person making request;
  Job title of the newcomers and workgroup;
  Start date;
  Services required (default services are: MS Outlook, MS Office and Internet access).

- Access to all Aquatic Control Engineering Limited systems is provided by our external IT provider (F5 Computing) and can only be started after proper procedures are completed.
- As soon as an individual leaves Aquatic Control Engineering Limited employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

11. Internal Access Control

- Access Control systems are in place to protect the interests of all users of Aquatic Control Engineering computer systems by providing a safe, secure and readily accessible environment in which to work.
- Aquatic Control Engineering will provide all employees and other users with the information they need to carry out their responsibilities in an as effective and efficient manner as possible.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner (ACE) and IT Services (F5 Computing). Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Every user should maintain the security of data at its classified level at all times.

- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the sensitivity/confidentiality of the data. Any data copied from company servers should only be taken from the business premises with the permission of the managing director.
- Users are obligated to report instances of non-compliance to the Information Security Officer or Managing Director
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made to the Managing Director.
- Users are expected to become familiar with and abide by Aquatic Control Engineering policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Information Security Policy and GDPR Policy.
- No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels.

## 12. Third party, online payment portal

Aquatic Control Engineering have an online payment system via the company website. The company website uses a third-party service provider; Stripe. Stripe has been audited by an independent PCI Qualified Security Assessor and is certified as a PCI Level 1 Service Provider. This is the most stringent level of certification available within the payments industry.

Stripe has its own security data protection process including encryption of sensitive data and communication. All card numbers are encrypted at rest with AES-256. Decryption keys are stored on separate machines. None of Stripe's internal servers and daemons can obtain plaintext card numbers but can request that cards are sent to a service provider on a static allow list. Stripe's infrastructure for storing, decrypting, and transmitting card numbers runs in a separate hosting environment, and doesn't share any credentials with Stripe's primary services (API, website, etc.).

Supporting Security information at Stripe can be requested from ACE's Information Security Officer and Managing Director.

Signed:

Stephen Randall
Managing Director