
# Angling Trust/Fish Legal

PD37 – AT/FL Information Security Polic

| DOCUMENT CONTROL | |
|---|---|
| **Version Number** | 2.3 |
| **Document Author** | Alistair Middleton |
| **Lead Director** | Simon Bourne |
| **Review Frequency** | Biennial |
| **Next Review Date** | Nov 2022 |
| **Purpose** | The Angling Trust handles sensitive data information daily. The purpose of this policy is to ensure that adequate safeguards are in place to protect data held and to ensure compliance with various regulations and to guard the future of the organisation. |

| REVISION HISTORY | | | |
|---|---|---|---|
| **Version** | **Date** | **Summary of Changes** | **Author** |
| 1.0 | Sept 2021 | New Document | COO |
| 2.0 | Jan 2017 | | |
| 2.1 | Nov 2018 | Updated Act details and inc GDPR | Alistair Middleton |
| 2.2 | Sept 2019 | Front Sheet updated. Font changed. Turquoise highlights corrected. | Alistair Middleton |
| 2.3 | Jan 2021 | Updated to reflect matters relating to COVID | Alistair Middleton |

| Approvals | | |
|---|---|---|
| **Approved by: CEO/COO/GOV COMM** | **Date** | **Version** |
| AT Board | Nov 2018 | 2.1 |
| | | |
| | | |
| | | |
| | | |

| Distribution | | | | |
|---|---|---|---|---|
| **Audience** | **Method** | **By whom** | **Date of issue** | **Version** |
| All Staff | Email/SharePoint | Gov Assistant | Jan 2021 | 2.3 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## CONTENTS

## 1. INTRODUCTION

This Policy Document encompasses all aspects of security surrounding confidential Angling Trust and Fish legal information. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy. All employees must read this document **(see table below for areas applicable in turquoise highlight)** and sign the form in **Appendix 1** confirming they have read and understand this policy fully. This document will be reviewed and updated by management on an annual basis or when relevant to include newly developed security standards into the policy and distributed.

| **Audience** | |
|---|---|
| Introduction | All staff |
| Information Security Policy | All staff |
| Acceptable Use Policy | All staff |
| Disciplinary Action | All staff |
| Protect Stored Data | All staff |
| Information Classification | All staff |
| Access to sensitive cardholder data | All staff |
| Physical Security | All staff |
| Data in transit | All staff |
| Disposal of stored data | All staff |
| Security Awareness and procedures | All staff |
| Network Security | SMT |
| System Password Security | All staff |
| Anti-Virus | SMT |
| Patch management | SMT |
| Remote Access Policy | All staff |
| Vulnerability management policy | SMT |
| Configuration standards | SMT |
| Change control | SMT |
| Audit log review | SMT |
| Penetration testing | SMT |
| Data Breach / Security incident response | All staff |
| Roles and responsibilities | All staff |
| Third party access to cardholder data | SMT |
| User Access Management | All staff |
| Wireless policy | SMT |
| | |
| Appendix A | All staff |

## 2. INFORMATION SECURITY POLICY

The Angling Trust handles sensitive data information daily. Sensitive Information must have adequate safeguards in place to protect them to ensure compliance with various regulations and to guard the future of the organisation.

The Angling Trust commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling Sensitive data should ensure:

- Handle Trust and member information in a manner that fits with their sensitivity;
- The Angling Trust reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Trust resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally.
-

We each have a responsibility for ensuring our Trust 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.

## 3. ACCEPTABLE USE POLICY

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to The Angling Trust's established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and The Angling Trust from illegal or damaging actions by individuals, either knowingly or unknowingly.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Keep passwords secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.

- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a Trust email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of The Angling Trust, unless posting is during business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

## 4. DISCIPLINARY ACTION

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

## 5. PROTECT STORED DATA

- All sensitive cardholder data stored and handled by The Angling Trust and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by The Angling Trust for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chat, messenger etc.,

**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.

## 6. INFORMATION CLASSIFICATION

Data and media containing data must always be labelled to indicate sensitivity level

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to The Angling Trust if disclosed or modified. **Confidential data includes cardholder data**.
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure;
- **Public data** is information that may be freely disseminated.

## 7. ACCESS TO THE SENSITIVE CARDHOLDER DATA

All Access to sensitive cardholder should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.

- Access rights to privileged user ID's should be restricted to least privileges necessary to perform job responsibilities
- Privileges should be assigned to individuals based on job classification and function (Role based access control)
- 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 they have a genuine business need.
- The Angling Trust will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
- The Angling Trust will have a process in place to monitor the PCI DSS compliance status any Service provider.

## 8. PHYSICAL SECURITY

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

- Keep physical passwords and entry keys to record areas secure and do not share, therefore strict control is maintained over the storage and accessibility of media
- 
- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on The Angling Trust sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.

## 9. PROTECT DATA IN TRANSIT

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, etc.).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

## 10. DISPOSAL OF STORED DATA

- All data must be securely disposed of when no longer required by The Angling Trust, regardless of the media or application type on which it is stored.
- All hard copies of cardholder data must be manually destroyed as when no longer required for valid and justified business reasons.
- All hardcopy materials must be crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- The Angling Trust will have documented procedures for the destruction of electronic media
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded”

## 11. SECURITY AWARENESS AND PROCEDURES

The policies and procedures outlined below must be incorporated into Trust practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Distribute this security policy document to all Trust employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A)
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Trust security policies must be reviewed annually and updated as needed.

## 12. NETWORK SECURITY

- Firewalls must be implemented at each internet connection and the internal Trust network.
- The Trusts IT provider must maintain a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the card holder data environment - must also be implemented to protect local network segments and the IT resources.
- All inbound and outbound traffic must be restricted to that which is required for the card holder data environment.
- All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented.
- All outbound traffic has to be authorized by management
- Disclosure of private IP addresses to external entities must be authorized.
- A topology of the firewall environment must be kept and updated by the Trusts IT provider. (rules, source IP, Destination IP action).
- No direct connections from Internet to cardholder data environment will be permitted. All traffic has to traverse through a firewall.

## 13. SYSTEM AND PASSWORD POLICY

All users, including contractors and vendors with access to The Angling Trust systems, are responsible for

taking the appropriate steps to select and secure their passwords.

- All users must use a password to access The Angling Trust network or any other electronic resources
- All user ID's for terminated users must be deactivated or removed immediately.
- The User ID will be locked out if there are more than 5 unsuccessful attempts.
- All system and user level passwords must be changed at least every 90 days.
- The responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:

a) Be as long as possible (never shorter than 6 characters).
b) Include mixed-case letters, if possible.
c) Include digits and punctuation marks, if possible.
d) Not be based on any personal information.

## 14. ANTI-VIRUS POLICY

- All machines must be configured to run the latest anti-virus software. The antivirus should have periodic scanning enabled for all the systems.
- The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, spyware and worms)
- All removable media should be scanned for viruses before being used.
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement of 3 months online and 1 year offline.
- End users must not be able to modify and any settings or alter the antivirus software
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

## 15. PATCH MANAGEMENT POLICY

- All Workstations, servers, software, system components etc. owned by The Angling Trust must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
- Where ever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors. Security patches have to be installed within one month of release from our IT Provider and have to follow a change control process.

## 16. REMOTE ACCESS POLICY

- It is the responsibility of The Angling Trust employees, contractors and 3rd parties with remote access privileges to The Angling Trust's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to The Angling Trust.
- Secure remote access must be strictly controlled. The Angling Trust will shortly be implementing two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.

- Vendor accounts with access to The Angling Trust network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.
- Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity
- All remote access accounts used by vendors or 3rd parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification.

## 17. VULNERABILITY MANAGEMENT POLICY

- As part of the PCI-DSS Compliance requirements, The Angling Trust will run internal and external network vulnerability scans bi-annual and after any significant change in the network (such as changes in network topology, firewall rule modifications,).
- Bi-annual internal vulnerability scans must be performed by The Angling Trust by our IT provider. All High vulnerabilities as defined in PCI DSS Requirement 6.2 are to be resolved immediately. All the vulnerabilities would be assigned a risk ranking such as High, Medium and Low based on industry best practices.

## 18. CONFIGURATION STANDARDS:

- Information systems that process transmit, or store card holder data must be configured in accordance with the applicable standard for that class of device or system.
- All network device configurations must adhere to The Angling Trust required standards before being placed on the network.
- Before being deployed into live use a new system must be certified to meet the applicable configuration standard required.
- All discrepancies will be evaluated and remediated by the IT provider.

## 19. CHANGE CONTROL PROCESS

- Changes to information resources shall be managed and executed according to a formal change control process between the Angling Trust and its IT provider. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.
- All change requests shall be logged whether approved or rejected on a standardised and central system. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.
- A risk assessment shall be performed for all changes and dependant on the outcome, an impact assessment should be performed.
- The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.
- All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.
- All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.

- All users, significantly affected by a change, shall be notified of the change. Users shall be required to make submissions and comment prior to the acceptance of the change.
- Implementation will only be undertaken after appropriate testing and approval by stakeholders.
- Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.
- All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

## 20. AUDIT AND LOG REVIEW

- This procedure covers all logs generated for systems concerning data over The Angling Trust network, including the following components:

    - Operating System Logs
    - Database Audit Logs.
    - Firewalls & Network Switch Logs.
    - File integrity monitoring system logs.

- Audit Logs must be maintained for a minimum of 3 months by IT Provider (available for immediate analysis) and 12 months offline.

- Agreed personnel are the only people permitted to access log files (i.e. COO, Business IT Manager).

- The following Operating System Events should be recorded and monitored: -
  a) Any additions, modifications or deletions of user accounts.
  b) Any failed or unauthorised attempt at user logon.
  c) Any modification to system files.
  d) Actions taken by any individual with root or administrative privileges.

- The following Database System Events are configured for logging, and are monitored by the network monitoring system (by IT provider)
  a) Any failed user access attempts to log in to the database.
  b) Any login that has been added or removed as a database user to a database.
  c) Any login that has been added or removed from a role.
  d) Any database role that has been added, changed or removed from a database.

- The following Firewall Events are configured for logging, and are monitored by the network monitoring system (by IT provider)
  a) ACL violations.
  b) Invalid user authentication attempts.
  c) Logon and actions taken by any individual using privileged accounts.
  d) Configuration changes made to the firewall (e.g. policies disabled, added, deleted etc)

- The following Intrusion Detection Events are to be configured for logging, and are monitored by the network monitoring system (by IT provider):
  a) Any vulnerability listed in the Common Vulnerability Entry (CVE) database.
  b) Any known denial of service attack(s).

c) Any authentication failure(s) that might indicate an attack.
d) Any traffic to or from a back-door program.

- For any suspicious event confirmed, the following must be recorded by the IT provider and the Angling Trust be informed
  a) User Identification.
  b) Event Type.
  c) Date & Time.
  d) Success or Failure indication.
  e) Event Origination (e.g. IP address).
  f) Reference to the data, system component or resource affected.

## 21. PENETRATION TESTING

- External intrusion tests will be performed remotely by our IT provider. Any audit team brought into the organisation by the Angling trust must to have access to the organisation's network.
- All the tests will be conducted from the equipment owned by the audit team so no equipment for the execution of the tests is required. The only requirement in this regard will be to have an active network connection for each member of the audit team. Those connections must provide access to the target network segment in every case.
- If an incident occurs during the execution of the tests that have an impact on the systems or services of the organization, the incident should be brought immediately to the attention of those responsible for incident management in the project
- It should be noted that in order to comply with PCI DSS the scope of the test should include, at least the following:

  1. Injections : Code, SQL, OS cmd, LDAP, XPath, etc.
  2. Insecure storage of cryptographic keys
  3. Insecure Communications
  4. Improper error handling
  5. Cross -site scripting (XSS)
  6. Control of inappropriate access.
  7. Broken authentication and incorrectly session management.
  8. Any other vulnerability considered High Risk by the organization.

- For all findings or vulnerabilities identified during the tests carried out will be generated and documented sufficient evidence to prove the existence of the same. The format of the evidence can be variable in each case, screen capture, raw output of security tools, photographs, paper documents, etc.
- As a result of tests performed should generate a document containing at least the following sections:

Introduction
Executive Summary
Methodology
Identified vulnerabilities
Recommendations for correcting vulnerabilities
Conclusions
Evidence

## 22. INCIDENT RESPONSE PLAN – DATA BREACH / SECURITY INCIDENT

**What is a personal data breach?**

*"a breach of security leading to the accidental, intentional or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service".*

**What is a security incident?**

*"a security incident' means any incident (accidental, intentional or deliberate) relating to our communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage our organisation.*

**Steps to take following a suspected or actual data breach / security incident:**

**Investigate the facts**

The data security breach should be investigated to determine:

- The nature and cause of the breach.
- The extent of the damage or harm that results or could result from the breach.
- Employees of the Trust will be expected to report to the Business and IT Manager and the Chief Operating Officer for any security related issues. For Fish Legal Penny Gale will be the initial point of contact.

**Stop or mitigate the breach**

Take action to stop the data security breach from continuing or recurring and mitigate the harm that may continue to result from the breach.

Any advice, instruction or direction will come from the Business and IT Manager and /or the Chief Operating Officer. For Fish Legal Penny Gale will be the initial point of contact.

*(N.B. If the ICO is notified or becomes involved in a data security breach, they will want to know what has been done to stop or mitigate the breach and what the data controller will do to ensure future compliance with Principle 7 of the Data Protection Act 1998 (DPA) (Security Principle*)

**Assess if a full incident team needs to be initiated**

If a data breach or security related incident is deemed severe either during an ongoing incident or from post incident closure (e.g. ICO or Audit recommendations) the Business Manager or Chief Operating Office can create and designate an 'incident response team' (IRT). This is a temporary structure and as an **example**: -

**Example Incident Response Team (IRT)**
Chief Operating Officer
Business and IT Manager
Governance Manager
Team manager applicable to incident
Director applicable to breach incident

*Note: The IRT team will be responsible for creating/updating and distributing an Incident Response Plan* (IRP).*

**Example Escalation – Second Level**
CEO
Board members

**External Contacts (as needed**)
ICO
IT Provider
IT System vendor
Internet Service Provider
Business Partners
Insurance

*The Incident response plan must be tested once annually. Copies of this incident response plan is to be made available to all relevant staff members and take steps to ensure that they understand it and what is expected of them

In response to a systems compromise, the IRT Response Team and designees will:

1. Ensure any compromised system/s is isolated on/from the network.
2. Gather, review and analyse the logs and related information from various central and local safeguards and security controls
3. Conduct appropriate forensic analysis of compromised system.
4. Contact internal and external departments and entities as appropriate.
5. Make forensic and log analysis available to appropriate parties or even law enforcement or card industry security personnel, as required.
6. Assist in any investigative processes, including in prosecutions.

**Determine the identity of the data controller(s)**

Determine the identity of the data controller for the purpose of the data security breach. The data controller is the party that determines the purpose for, and way personal data is processed.

There may be more than one data controller, particularly where, for example, shared services are involved. Where there is more than one data controller, both parties may be liable for the breach.

**Consider who needs to be notified**

The data controller will need to consider which parties should be notified. These could include:

**The ICO.** There is no express obligation in the Data Protection Act to notify the ICO in the event of a data security breach. However, the Information Commissioner believes that serious breaches should be brought to the attention of the ICO, so that the nature of the breach or loss can then be considered, together with whether the data controller is properly meeting his responsibilities under the DPA.

You need to consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO. If it's unlikely then you don't have to report it. The term "serious breaches" is not defined, but the ICO's examples of what would or would not be a serious breach include where:

- A large volume of personal data is involved and there is a real risk of individuals suffering some harm.

- The breach concerns information that if released could cause a significant risk of individuals suffering substantial detriment, including substantial distress. This is most likely to be the case where that data is sensitive personal data.

The ICO will want to know:

- What happened.
- When it happened.
- How it happened.
- How many people could be affected?
- What sort of data has been breached?
- What did you have in place that could have stopped it?
- What have you done to help the people this affects?
- What have you learned?
- How can you stop similar breaches in the future?

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

Responsibility for reporting to the ICO will be the Business and IT Manager and /or the Chief Operating Officer. For Fish Legal Penny Gale will be the initial point of contact.

**There many also be legal or contractual requirements to notify.**

- AT/FL data processing agreement
- Environment Agency contract
- Sport England contract
- Third party systems and services contracts (e.g. InFuse,)

**Data subjects**. The ICO cautions against the dangers of 'over notifying' data subjects, since not every incident will automatically warrant notification, and this may well cause disproportionate enquiries and work. Data controllers should instead consider how notification could help the individual, by allowing individuals to act

on the information to mitigate risks, for example by cancelling a credit card or changing a password. Data controllers may wish to consider providing data subjects whose personal data security is at risk with assistance in dealing with practical issues, such as identity fraud checking services. If notifying, the notification should at the very least include a description of how and when the breach occurred and what data was involved. Details of what the organisation has already done to respond to the risks posed by the breach should also be included.

**Post-incident contract review**

Consider whether the data security breach has been caused by another data controller (for example, where personal data has been made available to another data controller for the purposes of joined up or shared services) or whether it has been caused by a data processor. If so, consider whether there are contract terms in place.

Where the data security breach has been caused by a data processor, the data controller should consider their contract with the data processor, and in particular:

• Are the data protection and data security obligations in the contract appropriate?

• Does the breach give rise to a right to terminate the contract? In many contracts the breach of data security clauses will give rise to an express right to terminate.

• In the absence of an express right to terminate, consider whether the breach is sufficiently serious to give rise to the right to terminate the contract at common law for repudiatory breach. Whether such a right can be exercised will depend upon how serious the security breach is and its impact upon the parties' ability to continue to perform their contractual obligations.

• Are there are any specific contractual administration matters that need to be observed to preserve rights, such as compliance with notice provisions or prescribed alternative dispute resolution procedures?

**Does disciplinary action need to be taken?**

Data controllers will need to review the actions of employees who caused data security breaches and decide whether disciplinary action is appropriate. This will involve consideration of:

• The organisation's disciplinary policies and other relevant policies, such as data protection policies, IT and internet use policy and security policies to determine the extent to which the employee has breached their express contractual provisions.

• Whether the employee had received adequate training and guidance on data protection and security responsibilities and ought reasonably to have been aware of the employer's expectations and the consequences of breaching them.

**Audit of security appropriateness and the need to make necessary improvements**

An investigation should take place and include a review of whether appropriate security policies and procedures were in place and if so, whether they were followed.

**Complete Breach Register**

Enter the details of the data breach in the organisation's Breach Register, including information on actions taken post-incident.

**Best Practice**

- Take reasonable steps to use, maintain and upgrade any program which protects against computer viruses or any unauthorised use of or access to the Insured's computer system, network, electronic link or website
- Make secure back-up copies of any data, file or program at reasonably frequent intervals.
- Cancel any username, password or other security protection after the Insured became aware or had reasonable grounds to suspect that it had been made available to any unauthorised person;
- Take steps to ensure that all personal data held is encrypted.

## 23. THIRD PARTY ACCESS TO DATA

- All third-party companies providing critical services to The Angling Trust must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with The Angling Trust's Physical Security and Access Control Policy.
- All third-party companies which have access to Card Holder information must:

    1. Adhere to the PCI DSS security requirements.
    2. Acknowledge their responsibility for securing the Card Holder data.
    3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.

## 24. USER ACCESS MANAGEMENT

- Access to Angling Trust is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.
- The job function of the user decides the level of access granted.
- A request for service must be made in writing (email) 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
    Start date:
    Services required (default services are: Office 365 access):

- Access to all Trust systems is provided by IT and can only be started after proper procedures are completed.
- As soon as an individual leaves Angling Trust employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process HR will inform the IT provider of all leavers and their date of leaving.

## 25. ACCESS CONTROL POLICY

- Access Control systems are in place to protect the interests of all users of The Angling Trust computer systems by providing a safe, secure and readily accessible environment in which to work.
- The allocation of privilege rights (e.g. local administrator access) shall be restricted and controlled, and authorization provided jointly by the system owner.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- 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 data's classification
- Users are obligated to report instances of non-compliance to the Angling Trust.
- 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 in writing.
- Users are expected to become familiar with and abide by The Angling Trust policies, standards and guidelines

## 26. WIRELESS POLICY

- Installation or use of any wireless device or wireless network intended to be used to connect to any of the Angling Trust networks or environments is prohibited. If the need arises to use wireless technology, it should be approved by The Angling Trust and the following wireless standards have to be adhered to:

    1. Default SNMP community strings and passwords, passphrases, Encryption keys/security related vendor defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves The Angling Trust.
    2. The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
    3. Any other security related wireless vendor defaults should be changed if applicable.
    4. Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission

## 27. DISASTER RECOVERY / BUSINESS CONTINUITY / COVID 19

The Trust has a separate DR/BC plan which includes many section on IT and Information. This is updated frequently and distributed to managers, which is invoked in such an event to staff with an associated comms plan. This is largely about restoring services to an acceptable or agreed level of service as soon as possible.

**Covid 19**

Coronavirus (COVID-19) has substantially changed the working environment for the Angling Trust and all business across the country. Home-working, mandated by the UK Government wherever possible has been the trigger for this and will continue into the foreseeable future.

The primary implication of this is how the Trust deals payments by credit and debit card and we are required to comply with the Payment Card Industry Data Security Standard [PCI DSS].

There have always been existing specific requirements relating to **remote working** in existence for a long time now set out by the standards. However, the importance of these requirements is now coming to the fore.

The official guidance and "strengthening of emphasis" in these current times are detailed below:

**Policies and Procedures**

- To ensure compliance with policies and procedures, remote/home working staff need to be reminded of the security requirements related to payment card data. **These requirements are even more relevant in the current COVID-19 situation.**

- Policies and procedures need to be reviewed or updated to clearly prohibit any unauthorized copying, moving, sharing, or storing of payment card data in remote environments (e.g. the home).

- Remote staff additionally should also be aware of their physical surroundings, for example taking care to prevent sensitive information from being viewed by unauthorized persons (family members/friends)

**Risks**

Remote/home working can create some specific risks. These include:

1. Securing systems and data located in home-worker environments. This can be challenging and difficult to enforce. However, by limiting exposure of payment data in systems, scope and validation are simplified, reducing the chance of being a target for criminals. Examples of recommendations for key AT remote workers (membership team and competitions include):

    - Require all personnel to use only company-approved hardware devices, e.g. mobile phones, laptops, desktops, and systems. This is especially relevant to remote/at-home working, ensuring that Infuse and the Business and IT Manager of the Trust can maintain control of systems and technology supporting the processing of telephone-based payment card data.

    - Ensure that all desktop/terminals, in remote/at-home working environments:

      - Have personal firewalls installed and operational.
      - Have the latest version of the approved virus-protection software and definition files.
      - Have the latest approved security patches installed.
      - Are configured to prevent users from disabling security controls.

2. The physical environment within which an AT home worker is taking card payments over the telephone. This should be effectively monitored, and access controlled. Examples of required controls include:

    - Ensuring that at-home/remote workers use a multi-factor authentication process when connecting to AT systems or to any systems that process account data.
    - If account data is ever written or printed on paper, ensuring it is securely stored, then shredded when no longer needed.

**Conclusion**

Remote working requires the Angling Trust whom this is a relatively new situation to re-evaluate the security aspects of their activities. The requirements of the PCI DSS are not being relaxed, and, in fact, are needed more than ever.

**Specific PCI DSS requirements for Remote Working**

- Use multi-factor authentication for all remote network access originating from outside the company's network.
- Where passwords are used, enforce a strong password policy, and do not allow the use of shared passwords. Educate personnel on the importance of protecting their passwords from unauthorized access.
- Ensure all systems used by staff working remotely have up-to-date patches, anti-malware protection, and firewall functionality to protect from internet-based threats.
- Implement access controls to ensure that only individuals whose job requires access to the cardholder data environment (CDE), or cardholder data have access to those resources.
- Use only secure, encrypted communications—e.g., a properly configured VPN—to protect all transmissions to/from the remote device that contain sensitive information, such as cardholder data.
- Automatically disconnect remote access sessions after a period of inactivity, to avoid idle, open connections being used for unauthorized access.
- Ensure incident response plans are up to date and include accurate contact details for key personnel. Procedures for detecting and responding to a potential data breach could be different for incidents originating from remote work environments.

## Appendix A – Agreement to Comply with Information Security Policies for the Angling Trust

_____
**Employee Name (printed)**

_____
**Department**

I agree to take all reasonable precautions to assure that the Angling Trusts internal information, or information that has been entrusted to The Angling Trust by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with The Angling Trust, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in The Angling Trust security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

_____
**Employee Signature**

ANGLING TRUST FISH LEGAL