SECURITY POLICY

1. Introduction

The Financial Ombudsman Service (the Organisation) relies on the integrity and accuracy of its data in order to deliver a good service. This includes ensuring that the confidentiality, integrity and availability of the data is always maintained. Any third party organisation that processes, manages or interacts with this data must adhere to these principals to ensure that the trust of our consumers is maintained.

2. Purpose

This document sets out the minimum information security requirements expected of third parties who have access to the Organisations' information during the provision of contracted services. The Policy aims to effectively protect information and data by providing a flexible yet consistent approach to managing information security risk in third party suppliers, and assist the suppliers to better understand and work co-operatively with the Organisation on proportionate security controls.

3. Scope

The scope of this Policy includes any third party which will have access to or process the Organisations data. This includes, but is not limited to:

- All third party suppliers involved in the processing of data as defined by the Data Protections Act 2018
    - Access to the Organisations data from any remote locations where the network and computers are not under the control of the Organisation
    - Any users who are not employees of the Organisation and require or have access to the Organisations data

This Policy therefore also applies to all staff, including contractors, temporary staff and third parties employed directly and indirectly by the Third Party organisation (e.g. subcontractors or "fourth" parties).

If there is a direct conflict between any requirements of this Policy and the terms of a written contract or agreement between the Supplier and the Organisation, then the terms of the written contract or agreement will prevail.

4. Information Security Policy

The Third Party shall at all times maintain a management-approved corporate Information Security Policy, or set of Information Security Policies, defining responsibilities and setting out the Third Party's approach to information security.

A supporting framework of policies and security plan covering all requirements set out in this document in line with industry best-practice will be maintained at all times.

The Information Security Policies will be published and effectively communicated to all staff responsible for the Organisations Information.

The Third Party shall at all times ensure that its Information Security Policies are assigned to a responsible owner, and are maintained, monitored and reviewed on a scheduled basis to deliver continuous improvement.

5. Third Party Organisation

The third party shall designate named individuals or teams who will have responsibility and accountability for all information security policies, implementation and processes. Such nominated individuals shall act as the primary points of contact where information security is concerned including incident management. Additionally they shall facilitate any security review audit meetings and manage any restoration plan in the event of a security breach or event which affects the availability of the service.

The Third Party senior management shall provide clear strategic direction and support business areas to assess monitor and control information security risks, and ensure that information security issues raised are properly addressed.

6. Compliance and Legislation

The Third Party shall not process or otherwise use the organisations data, for any purpose other than that which is directly required for the supply of the agreed Services.

The Third Party shall not purport to sell, let for hire, assign rights in or otherwise dispose of any data without the prior written approval of the Organisation.

Acceptable usage policies must be defined and communicated to all Third Party employees and subcontractors. The policies must cover:

- Handling and accessing the Organisations data
- Appropriate usage of internet, email and telephones
- Change control
- Incident reporting
- Data Protection Act 2018
- Computer Misuse Act 1990

7. Human Resources and Staff Vetting

The third party shall ensure that all roles and responsibilities relating to the security, processing and interaction of all the third party employees are clearly defined, documented and communicated.

A clear employee code of conduct, disciplinary policy and procedures should be in place. The policy should clearly define what is and isn’t acceptable as well as what constitutes a security breach or an incident.

The Third Party must ensure that staff vetting procedures equal to or exceeding those stipulated in Appendix A are utilised for all employees.

The Third Party shall ensure that all employees enter into a written contract of employment under which they agree to adhere to all Third Party policies, rules and procedures including all information protection policies and agree to assign all intellectual property created in the course of providing the Services to the Third Party so that the intellectual property provisions of the Contract can take effect.

Formal disciplinary procedures must be in place for employees and Subcontractors who breach any applicable security policy related to the protection of information or data.

8. Training and Awareness

The Third Party will define a security training and awareness campaign focusing on knowledge of fraud and security issues, as well as the risks resulting from poor information security. This will include the legal and regulatory obligations including the responsibilities of Third Party personnel and its Subcontractors throughout the provision of the services.

The Third Party shall ensure that all Third Party personnel (including Subcontractor personnel) have the appropriate skills and training to support the Services, and that all IT or Information Security personnel (including Subcontractor personnel) have been given the authority and training to appropriately discharge their responsibilities.

9. “Fourth parties” and Sub-contractors

The Third party shall not assign, sub-contract or in any other way dispose of the Contract or any part of it without the Ombudsman's prior Approval. Sub-contracting any part of the Contract shall not relieve the Contractor of any of its obligations or duties under the Contract.

If the Third Party utilises subcontractors then agreement from the Organisation must be obtained. Full details of any Subcontractor(s) used in the provision of the Services will be provided; such details to include as a minimum company name, address, location, and type of Services to be provided and the volume.

The Third Party shall establish and at all times maintain safeguards against the accidental or deliberate or unauthorised disclosure, access, manipulation, alteration and against any destruction, corruption of, damage, loss or misuse of the Organisations data in the possession of the Third Party or any sub-contractors or agents of the Third Party.

The Third Party shall conduct annual security reviews of the Subcontractors where those Subcontractors have access to the Organisations information, and maintain detailed, written evidence of these audits to include any security risks, recommendations and remedial actions.

10. Malware and Anti-Virus Protection

The Third Party shall ensure that anti-virus and anti-malware software is installed on all Third Party Systems vulnerable to virus infection and shall ensure that its Subcontractors shall do the same. The Third Party shall (and shall ensure that its Subcontractors shall) use all possible measures to detect malicious or hidden code that is designed to, or will have the effect of:

- destroying, altering, corrupting or facilitating the theft of any Information or data
- disrupting, disabling or removing any software
- using undocumented or unauthorised access methods for gaining access to systems or Information

The Third Party shall ensure that anti-virus and anti-malware software and definition files are updated for all Third Party Systems in line with vendor recommendations and industry standards. The Third Party shall also ensure that its Subcontractors shall do the same on any Subcontractor systems used in the provision of any service.

The Third Party shall promptly notify the Organisation in writing as soon as it becomes aware of any viruses in any of the Third Parties Systems or Systems, directly (or indirectly) affecting the Organisation. This is considered an incident.

A written report will be provided to the Organisation describing the incident, the measures that were taken to resolve the incident and what measures were taken to prevent any reoccurrence.

11. Patching

The Third Party shall ensure that all software and systems utilised or involved in the delivery of services, data processing or storage of the Organisations data are patched in-line with the vendor recommendations or industry standards. Or patched as soon as practicable if the Third party assesses the need as urgent such as high profile or media interest where vulnerabilities are being actively exploited.
Appropriate steps shall be taken to ensure that all patches are tested or reviewed prior to deployment to minimise disruption to live services. A patching timetable should be agreed with the Organisation and documented in Appendix B.

12. Database Security and Data Segregation

The Third Party must agree with the Organisation the requirements for data and database segregation prior to usage and documented in Appendix B.

All Organisational data must be securely sandboxed or segregated from other system or service users or customers.

Where the Third Party is processing or storing data sets relating or provided by employees or consumers then the data must be stored or processed in a way which ensures segregation from other data sets.

13. Security of network services

The Third Party must ensure protection of information in networks by maintaining physical and logical security network equipment, implementing and managing network firewalls on network interfaces and security equipment configuration data to prevent intrusion.

14. Secure Development

A policy outlining a secure process for the development of software, code and systems processing the Organisations data or Information, whether in-house or outsourced, needs to be defined and maintained. This policy must align to the OWASP guidance as well as any other industry standards.

The Third Party shall ensure that change control procedures are agreed and documented between the Third Party and the Organisation to include the following:

- why the change was required
- how and when the changes will be executed
- what the impact will be
- what testing has or will be conducted
- Define and maintain an acceptance criteria for any new systems, upgrades, new versions and patching of systems.

Any emergency changes will also require agreement from the Organisation.

The Third Party shall notify the Organisation of any upgrades or configuration changes which will impact on the security of any systems or services that are of relevance to the Organisation.

The Third Party shall ensure that back out procedures are documented prior to implementing any change.

15. Data Encryption

The Third Party must ensure that any data deemed to contain classified, sensitive or personal data and collected, stored or processed on behalf of the Organisation must be encrypted at all times whilst at rest using approved encryption algorithms and protocols. This also includes during the data transfer process.

The Third Party must inform and gain approval from the Organisation of its intended use of cryptography and use protocols documented in Appendix B.

16. Secure Backups

The Third Party shall ensure that regular backups of all Third Party Systems hosting the Organisations information are performed. Testing of restoration capabilities must be carried out on a periodic basis in-line with industry standards and vendor recommendations.

The Third Party shall ensure that where backups are stored off-site they are always securely transported and encrypted, with a register of all backup media maintained.

17. Technical Security

Technical security policies and standards for applications and systems used in processing collecting and storing the organisations data and information must be defined, documented and maintained.

All policies and standards must be in-line with industry standards and vendor recommendations.

The Third Party shall ensure that regular penetration and/or vulnerability testing is carried out and shall agree in writing beforehand the scope of penetration testing with the Organisation.

18. Email and Data Transfer

All transfers of data including e-mail, direct transfer and via removable or writable media must be secured appropriately.

The methods for transfer must be agreed with the Organisation prior to transfer and documented in Appendix B.

19. Access Control including Remote Access

The Third Party shall always maintain the confidentiality, integrity, and availability of the Organisations information and data through the use of appropriate access controls.

The Third Party shall have a documented procedure for the provision and access to all systems utilised in the provision of services or data processing and storing of the Organisations data.

Access will be limited to those personnel that need access to such information or systems to perform their duties. This includes the provisioning of temporary and guest accounts as well as any system providing remote access or wireless functionality.

The Third Party shall have a defined password and user account policy that meets or exceeds the following principles:

- defined minimum password length in-line with industry standards
- defined minimum password complexity in-line with industry standards
- minimum and maximum age and password reuse prevention
- defined password lockout in-line with industry standards

Automated session timeouts (e.g. lockouts, logouts) must be enforced automatically after a period of inactivity in line with industry standards on devices accessing FOS information.

20. Physical Security

The Third Party must ensure that only authorised personnel have access to any buildings or premises used for the storage or processing of any of the Organisations data or information. This includes the provisioning of temporary and visitor access as well.

Appropriate physical security controls must be in place at all times.

The Third Party must ensure that appropriate protection for the mitigation of damage by fire or floods is utilised and tested in-line with industry standards.

21. Business Continuity and Disaster Recovery

The Third Party shall ensure that a Business Continuity (BC) Plan exists in relation to the provision of systems or services to the Organisation. The plan shall set out how services and operations shall be restored following any incident or event considered severe enough to disrupt or cause the failure of business processes within a time period agreed with the Organisation.

22. Off-boarding and Contract Exit Considerations

The Third Party must ensure that all Organisational data is available in a usable format at the point of contract termination at no additional cost to the Organisation.

Secure deletion and destruction of all Organisational data adhering to HMG **CSEG IS5 or BS EN 15713** standard using products that are CESG CPA certified must be possible at the point of contract termination at no extra cost to the Organisation. The third party supplier must provide the Financial Ombudsman Service with a certificate of destruction for each asset.

On or after termination of the Services, the Third Party shall grant the Organisation the right to perform appropriate audits to ensure compliance by the Third Party under the terms of the contract.

23. Incident Management

The Third Party shall always maintain and utilise a security incident response procedure at all times.

If the Third Party becomes aware of a security incident that directly, or indirectly affects the Organisation then it must:

- Immediately report the incident
- Promptly provide the Organisation with a high level report of the incident including the cause, impact and nature of the data involved
- Take immediate action to contain the incident and prevent any further occurrences

A written report will be provided to the Organisation describing the incident, the measures that were taken to resolve the incident and what measures were taken to prevent any reoccurrence of the incident within 48 hours of incident identification. The written report will highlight any Organisational data that might have been affected. It will also include details of any suspected or confirmed criminal activity.

24. Logging and Auditing

The Third Party must ensure that all systems and services used for the processing, storing and collecting of the Organisations data are capable of full usage audit. This includes the audit of any administrative functions associated with the service or systems.

The Third Party must retain the audit logs for a period agreed with the Organisation.

25. Third Party Auditing Requirements

The Third Party shall grant the Organisation the right to perform reasonable audits and inspections of the Third Party and its Subcontractors to ensure, but not limited to the compliance with this contract. Any evidence requested shall be provided to the Organisation within a reasonable time period.

A notice period of 48 hours will be given to the Third Party to facilitate an audit. Failure to facilitate the audit after 48 hours will be deemed as breach of this contract.

Appendix A to Schedule 1: Staff Vetting Procedures

It is consistent with the Data Protection Act 2018 that an individual's refusal to undergo an essential check where there are no alternatives could lead to a refusal of employment. In such cases, individuals should be made aware that it will not be possible to take them on, should they refuse.
There are 5 main elements to the Staff Vetting Procedure for external contractors:

- Verification of identity and address
- Proof of right to work in the UK
- Verification of employment history
- Address checks
- Criminal record checks for unspent convictions

Verification of Identity and address
Verification of identity is essential before any individual can begin their employment. Identity can be verified by physically checking a range of appropriate documentation.

Only original documents should be used for identification purposes. Copies are not appropriate.

Verification of identity should be achieved by checking a Current signed full passport. Verification of address can be achieved by checking 1 of the following documents which must have been issued in the past 6 months:

- Proof of residence from a financial institution.
- Recent original utility bill or certificate from a utility company confirming the arrangement to pay for the services at a fixed address on prepayment terms
- Local authority tax bill (valid for current year)
- Bank, building society or credit union statement or passbook containing current address
- Recent original mortgage statement from a recognised lender
- Court order

Verification of right to work
Confirmation of permission to work in the UK must be carried out prior to the commencement of employment.

Verification of Employment History
To ensure that prospective employees are not concealing associations or gaps, employing departments and agencies should, as a minimum, verify recent (past 3 years) employment or academic history.

Criminal record checks for unspent convictions
All employees should undergo a check for "unspent" criminal records with details of any unspent convictions being provided to the Ombudsman for consideration.

Under the terms of the Rehabilitation of Offenders Act 1974, it is reasonable for employers to ask individuals for details of any "unspent" criminal convictions. The Act states that if an offender remains free of further convictions for a specified period (the "rehabilitation period") the conviction becomes "spent".

Disclosure and Barring Service (DBS) offers a check of “unspent‟ criminal records through its Basic Disclosure service. Basic Disclosure Certificates contain details of convictions considered “unspent” under the Rehabilitation of Offenders Act 1974.
Where an individual provides his or her own Basic Disclosure, the Contractor should ensure the validity of the documentation.

Appendix B to Schedule 1 – Supplier's Technical Controls

Contractual Points for Negotiation:

The following sections must be negotiated or clarified prior to contract signing.

9. The use of third parties must be identified and agreed
11. The patching timetable should be agreed
12. Segregation methods must be identified and agreed
14. The Encryption methods must be agreed
17. Data transfer methods must be identified and agreed
23. Audit logging requirements and log retention must be agreed