# NSPCC - Supplier Security Assessment

## Introduction

The purpose of this document is to establish the information security credentials of a supplier so the NSPCC can perform a risk assessment on the service offering.

The document should be completed by the following people:

* The supplier providing the service to the NSPCC.
* The NSPCC Security manager reviewing the response.

***Please note, GDPR legislation is now active legislation and its compliance is mandatory for data controllers and processors by May 2018. From May 2018 onwards compliance failures may result in hefty penalties to data processors who have not implemented appropriate technical and organisational measures. Therefore the NSPCC expects its suppliers who process personal data on its behalf to be taking active steps to become GDPR compliant by this deadline. The NSPCC reserves the right to issue a subsequent security assessment at a later date to determine the supplier’s GDPR compliance.***

Note, the NSPCC may choose to audit the supplier’s response to this document.

## Supplier Details

In this section please provide details of the supplier and the service offered to the NSPCC.

|  |  |
| --- | --- |
| The name of the supplier. |  |
| The name and the role of the person completing this assessment. |  |
| Contact details for the supplier. e.g. phone, email, website, company registration number. |  |
| The service the supplier intends to provide. |  |
| The classification of the information that would be in the supplier’s possession.* **Confidential** – Sensitive information such as personal data (name, address, phone number, age, etc.), child case notes, photographs of targeted individuals, etc.
* **Internal** – Information such as emails, plans, reports, etc.
* **Public** – Information taken from the public domain.
 |  |
| The name of the NSPCC department that has requested this service. |  |
| The time when the service will start and finish. |  |
| The date the supplier completed this assessment. |  |

## Supplier Security Assessment

This section needs to be completed by the supplier to gauge their security position. If a question is not relevant then enter Not Applicable (“NA”). Please provide comments for responses that are either “No” or “NA”.

| Item | Security Question | Yes/No | Comments |
| --- | --- | --- | --- |
| Q1 | Does the supplier have a defined security policy?  |  |  |
| Q2 | Is the supplier registered under the UK Data Protection Act? If yes then provide the reference. |  |  |
| Q2b | Is the supplier aware of their responsibilities under GDPR legislation and actively taking steps to become GDPR compliant by May 2018? |  |  |
| Q3 | Is the supplier accredited to a recognized security standard? |  |  |
| Q4 | Will any confidential data be stored outside of the EU as part of this service? If yes then describe the security arrangements. |  |  |
| Q5 | Are staff made aware of their information security responsibilities? |  |  |
| Q6 | Does the supplier vet new staff and ensure leavers have their access rights removed? |  |  |
| Q7 | Will the supplier ensure that when sensitive information is exchanged with the NSPCC that this is done securely? e.g. encrypted email, password protected documents, HTTPS protected websites, Secure FTP, etc. |  |  |
| Q8 | Will the supplier remove our data from their computer systems once the engagement is completed? |  |  |
| Q9 | Does the supplier use legitimate and vendor supported software? |  |  |
| Q10 | Does the supplier protect its computers and network with anti-malware products? |  |  |
| Q11 | Does the supplier require the use of complex passwords to access their computers? |  |  |
| Q12 | Does the supplier regularly patch their computer operating systems? |  |  |
| Q13 | Are portable devices (laptops, smart phones, USB flash drives, etc.) protected by encryption? |  |  |
| Q14 | Does the supplier use firewall(s) to protect its internal computers from the Internet? |  |  |
| Q15 | Does the supplier use a solution to backup and restore their computer systems in the case of failure? If yes then please describe. |  |  |
| Q16 | Does the supplier have physical building security to protect its information systems? |  |  |
| Q17 | Will the supplier report any information security incidents impacting the NSPCC as soon as possible? |  |  |
| Q18 | Please describe any additional security controls the supplier has in place. |  |  |

## NSPCC Security Recommendation

This section should be completed by the NSPCC Security Manager after the supplier has provided the information above.

|  |  |
| --- | --- |
| The name of the Security Manager |  |
| The details of the security recommendation. |  |
| Should we proceed with this supplier? |  |
| The date the recommendation was completed. |  |

## Appendix - Supplier Security Principles

The NSPCC has an expectation when working with a supplier that they adhere to a common set of security principles which are listed below. This helps the NSPCC assess the risk of working with a supplier. Where a supplier does not follow these principles then this should be highlighted to the NSPCC.

**Security policy** - The supplier should have a documented security policy that outlines the security controls the company adheres.

**Personnel security** - The supplier is responsible for ensuring staff are made aware of their contractual and information security responsibilities. The supplier should ensure they operate a defined starters and leavers process. The supplier should monitor staff conformance and take appropriate measures when these are found deficient.

**Physical security** - The supplier should use physical and environmental security to protect its offices and information systems.

**Operations security** - The supplier is responsible for ensuring services they deliver to the NSPCC are properly managed in terms of service delivery such as incident, problem and change management. Information systems used in the delivery of their services should be on vendor supported operating systems, configured securely, patched, protected from malware, resilient, auditable, and backed up to minimize service interruption to the NSPCC.

**Communication security** - The supplier should ensure that communications with the NSPCC involving sensitive information are performed securely and are kept confidential.

**Supply chain** - The supplier is expected to have appropriate agreements in place to ensure services provided by sub-contractors do not expose the NSPCC to an adverse level of risk.

**Compliance** - The supplier is expected to comply with legislative, regulatory and contractual requirements. Personal data should be handled as defined under the data protection act. Sensitive information encountered by the supplier whilst working for the NSPCC should be kept confidential and not disclosed. Suppliers who connect directly into the NSPCC's network must comply with the NSPCC's security policy.

**Security incidents** - The supplier should report any security incidents impacting the NSPCC immediately and take the appropriate actions to contain, eradicate and recover from the incident.