**Introduction**

NatCen’s information security policy requires an evaluation of third parties who process, handle or store NatCen information. This questionnaire should be completed by the person responsible for information security within the organisation being contracted to provide services to NatCen.

The objective of the process is to understand any data security risks associated with the provision of the services. It may be necessary to discuss any aspects that may compromise the protection of data.

This questionnaire consists of two columns, one with the question posed to you, the second for your response. If the question does not apply to the services that are to be provided, then an “N/A” in the answer response column is sufficient.

**General information**

|  |  |
| --- | --- |
| * 1. Company name and address
 | Click or tap here to enter text. |
| * 1. Company website
 | Click or tap here to enter text. |
| * 1. Information security contact
 | Name. |
| Email address. |
| Phone number. |
| * 1. Please provide a brief description of service to be provided to NatCen.
 | Click or tap here to enter text. |
| * 1. What information will or does the organisation process, handle or store on behalf of NatCen? Does this include personal details such as name and address?
 | Click or tap here to enter text. |
| * 1. On what types of system will you store the data? (e.g. server on premises, cloud, local devices)
 | Click or tap here to enter text. |
| * 1. Will you store and process all our data in the UK only? If not, in which countries will our data be stored and processed?
 | Choose an item.Click or tap here to enter text. |
| * 1. At which locations will you store and process data for NatCen?
 | Click or tap here to enter text. |
| * 1. Do you own or manage this environment? If not, please list who does.
 | Choose an item.Click or tap here to enter text. |
| * 1. Are you certified to any information security or quality standards such as ISO 27001 or ISO 9001, or do you have any alternative certification such as PCI DSS? If so please state the scope for these certifications.
 | Choose an item.Click or tap here to enter text. |

**Policy and awareness**

|  |  |
| --- | --- |
| * 1. Do you have a formal information security policy? If so, please provide a copy.
 | Choose an item.Click or tap here to add any additional information. |
| * 1. Is the policy formally approved by senior management and regularly reviewed?
 | Choose an item.Click or tap here to add any additional information. |
| * 1. Who is responsible for monitoring compliance to the information security policy?
 | Click or tap here to enter text. |
| * 1. How do you promote awareness of the policy for both staff and contractors?
 | Click or tap here to enter text. |
| * 1. Do you ensure that specific information security and data protection training is provided regularly (at least annually) to your employees, contractors and temporary staff?
 | Choose an item.Click or tap here to add any additional information. |

**Human Resources security**

|  |  |
| --- | --- |
| * 1. Please describe any screening or vetting processes that you carry out on employees and third parties.
 | Click or tap here to enter text. |
| * 1. Are all personnel required to sign non-disclosure and/or confidentiality agreements?
 | Choose an item.Click or tap here to add any additional information. |
| * 1. What disciplinary process do you have to ensure that any intentional misuse of information is managed for employees or sub-contractors?
 | Click or tap here to enter text. |
| * 1. Describe your leaver process or policy in terms of revoking access, retrieving equipment or information, and ongoing responsibilities of individuals regarding non-disclosure.
 | Click or tap here to enter text. |

**Sub-contractors**

|  |  |
| --- | --- |
| * 1. Will/do you allow any sub-contractors, including cloud providers, to have access to NatCen data?
 | Choose an item.Click or tap here to add any additional information. |
| * 1. If Yes to 1, do you have prior written consent from NatCen for any information processing by sub-contractors?
 | Choose an item.Click or tap here to add any additional information. |
| * 1. Do all of those sub-contractors store and process data in the UK only? If not, in which other countries?
 | Choose an item.Click or tap here to enter text. |
| * 1. Is IT support and maintenance of your IT system carried out by your employees or is it sub-contracted?
 | Choose an item.Click or tap here to add any additional information. |
| * 1. Do you have agreements or contracts in place to ensure that data protection and security arrangements meet NatCen security requirements?
 | Choose an item.Click or tap here to add any additional information. |
| * 1. Do you audit your sub-contractors?
 | Choose an item.Click or tap here to add any additional information. |

**Physical security**

|  |  |
| --- | --- |
| * 1. Describe the security controls protecting the locations where the information is being stored or processed (e.g. physical entry arrangements, video monitoring, visitor access controls).
 | Click or tap here to enter text. |
| * 1. Can a representative from NatCen visit your facilities to observe the physical security controls in place? (announced or unannounced)
 | Choose an item.Click or tap here to add any additional information. |
| * 1. Will NatCen information be transferred to hard copy? If so what and how much?
 | Choose an item.Click or tap here to enter text. |
| * 1. If Yes to 3: do you have a clear desk policy which states that papers containing sensitive data (including NatCen information) must not be left unattended on desks for long periods or overnight?
 | Choose an item.Click or tap here to add any additional information. |

**Operational controls - change and incident management**

|  |  |
| --- | --- |
| * 1. Are changes to any of your systems that hold NatCen information tested, reviewed and applied using a documented change management process? Please describe.
 | Choose an item.Click or tap here to enter text. |
| * 1. Do you have an incident management process that is documented, approved and monitored?
 | Choose an item.Click or tap here to add any additional information. |
| * 1. Do you have a procedure for reporting incidents of information loss, breach of confidentiality or integrity to NatCen? If so, please describe.
 | Choose an item.Click or tap here to enter text. |
| * 1. Do you have a process for dealing with incidents that require forensic investigation?
 | Choose an item.Click or tap here to add any additional information. |

**Risk assessment and asset management**

|  |  |
| --- | --- |
| * 1. Do you undertake regular security risk assessments and take steps to mitigate the risks identified? If so, please describe the process as it affects NatCen information.
 | Choose an item.Click or tap here to enter text. |
| * 1. Do you maintain an inventory of assets?
 | Choose an item.Click or tap here to add any additional information. |
| * 1. Do you have an information classification process? If so, how is it applied to NatCen information held, accessed and processed by you?
 | Choose an item.Click or tap here to enter text. |
| * 1. Is device encryption in place on servers, PCs and laptops that are or will be used to access or store confidential NatCen information? If so, describe the standard of encryption that applies to each. Whole disk encryption to the FIPS 140-2 standard is required for all mobile devices.
 | Choose an item.Click or tap here to enter text. |
| * 1. Is access to NatCen information on your systems permitted only from corporate encrypted laptops, or do you operate a Bring Your Own Device (BYOD) policy? If BYOD, how is security managed?
 | Click or tap here to enter text. |
| * 1. What removable media is allowed and what can it access? (e.g. all USB devices with data capability are blocked)
 | Click or tap here to enter text. |
| * 1. Will NatCen information be transferred to or stored on removable media such as USB memory devices? If so, please describe your arrangements for protecting such information from corruption, loss or disclosure including details of the security tools and the standard of encryption applied.
 | Choose an item.Click or tap here to enter text. |
| * 1. If Yes to 7, what procedures do you have for the handling and management of removable media containing NatCen information and hard copy information in transit and storage?
 | Click or tap here to enter text. |
| * 1. Will NatCen information be held or stored locally on laptops or PCs? If so, are those devices protected from corruption, loss or disclosure using encryption? Please describe your arrangements including details of the security tools and the standard of encryption applied.
 | Choose an item.Click or tap here to enter text. |
| * 1. What backup systems, if any, are in place for NatCen information?
 | Click or tap here to enter text. |
| * 1. Is the backup encrypted?
 | Choose an item.Click or tap here to add any additional information. |
| * 1. Is there any off-site storage for backups? If so, where are those backups stored and how are they secured?
 | Choose an item.Click or tap here to enter text. |
| * 1. What procedures and mechanisms do you use for controlling and disposing of paper documents containing NatCen sensitive data?
 | Click or tap here to enter text. |
| * 1. How will you delete the data you receive from NatCen?
 | Click or tap here to enter text. |
| * 1. Are you able to carry out secure deletion of our data to the US DoD (7-pass) standard?
 | Choose an item.Click or tap here to add any additional information. |
| * 1. What is your process for destroying obsolete or damaged machines and disks? Does the secure destruction of redundant equipment and media include the secure erasure of NatCen information?
 | Click or tap here to enter text. |
| * 1. Do you have an active Business Continuity / Disaster Recovery policy or process in place? If so, how often is an exercise carried out?
 | Choose an item.Click or tap here to enter text. |
| * 1. Do you use Machine Learning or Generative Artificial Intelligence (AI) models in any services provided to clients or is client data otherwise exposed to AI models?

Answer yes if Machine Learning or Generative AI models are used anywhere within the services provided to your clients or anywhere that might touch client data. This includes the use of AI features or capabilities embedded in your suppliers’ services or any SaaS tools your people may use (e.g. Google Gemini or Microsoft's Copilot), if they are used with client data to provide client services. If AI is used within some, but not all of the services you provide, you should answer yes. Please describe which of your services use AI and a brief description of where and how AI is used in each service. | Choose an item.Click or tap here to enter text. |

**Technical controls**

Segregation of information between customers

|  |  |
| --- | --- |
| * 1. What security controls are in place to keep NatCen data separate from other customers’ data?
 | Click or tap here to enter text. |

Access control

|  |  |
| --- | --- |
| * 1. How often do you review user access to ensure that members of staff continue to have only the minimum access to NatCen information and systems they require for their current role?
 | Click or tap here to enter text. |
| * 1. Are all computers to be locked by a password when left unattended? Do you have a formal policy which enforces this?
 | Choose an item.Click or tap here to enter text. |
| * 1. Do you use multi-factor authentication (MFA), also known as 2-step verification (2SV), to mitigate against password guessing and theft? If so, please describe how it is implemented.
 | Choose an item.Click or tap here to enter text. |

Operating System security

|  |  |
| --- | --- |
| * 1. Do you have IS procedures for protecting your systems against vulnerabilities?
 | Choose an item.Click or tap here to add any additional information. |
| * 1. Do you perform regular vulnerability scanning of your customer environment? If so, what tools are used?
 | Choose an item.Click or tap here to enter text. |
| * 1. Do you have a patch management process? Please describe.
 | Choose an item.Click or tap here to enter text. |
| * 1. Is anti-virus software deployed on servers and on laptops, PCs and other devices that have access to NatCen data? If so, please name the products used.
 | Choose an item.Click or tap here to enter text. |
| * 1. How often are virus definitions updated?
 | Click or tap here to enter text. |
| * 1. Are email filtering and web browsing malware prevention in use? Please describe.
 | Choose an item.Click or tap here to enter text. |

Network security

|  |  |
| --- | --- |
| * 1. Are firewalls used to protect your systems and data from the internet and other untrusted networks? Please name the devices.
 | Choose an item.Click or tap here to enter text. |
| * 1. Are intrusion detection/prevention systems used? Please name the devices.
 | Choose an item.Click or tap here to enter text. |
| * 1. Are security logs monitored to detect malicious activity?
 | Choose an item.Click or tap here to add any additional information. |
| * 1. Will wireless technology be used in this environment? If so, how is this protected?
 | Choose an item.Click or tap here to enter text. |
| * 1. Is penetration testing carried out and if so how often?
 | Choose an item.Click or tap here to enter text. |

Remote working

|  |  |
| --- | --- |
| 1. Are home and/or mobile working in place? If so, how are the risks assessed?
 | Choose an item.Click or tap here to enter text. |
| 1. What technology is used to allow home/remote working (e.g. VPN, DA) and what standard of encryption is applied to data in transit?
 | Click or tap here to enter text. |
| 1. Is there remote access capability from non-corporate devices?
 | Choose an item.Click or tap here to add any additional information. |

**Compliance**

|  |  |
| --- | --- |
| * 1. Can you confirm that all services or systems processing NatCen information are compliant with all relevant statutory, regulatory, contractual, copyright and intellectual property requirements?
 | Choose an item. |
| * 1. Are you registered with the Information Commissioner's Office (ICO) under the Data Protection Act 2018? If yes, state your registration reference.
 | Choose an item.Click or tap here to enter text. |
| * 1. Can you confirm that all NatCen information containing personal information will be handled in accordance with UK Data Protection legislation?
 | Choose an item. |
| * 1. Have you ever had to report a breach to the Information Commissioner’s Office (ICO)? (If yes please provide further information)
 | Choose an item.Click or tap here to enter text. |
| * 1. Has the ICO issued any assessments against you or required an undertaking to be signed? (If yes please provide further information)
 | Choose an item.Click or tap here to enter text. |
| * 1. Please describe the processes in place to ensure the ongoing monitoring of your information security arrangements.
 | Click or tap here to enter text. |

**continued**

**Declaration**

**Signed undertaking**

This document is signed in acceptance that the signatory’s organisation, and any other organisations accessing NatCen assets on behalf of the contractor, comply with statements made in this document.

**Senior Officer(s) for the contractor with responsibility for information security**

|  |  |
| --- | --- |
| **Signed:** | Click or tap here to enter text. |
| **Print name:** | Click or tap here to enter text. |
| **Position in organisation:** | Click or tap here to enter text. |
| **Date:** | Click or tap to enter a date. |