

**Nottingham City Council**

**IT Services**

**IT Security Review**

**Questionnaire**

**Version 1.3**

|  |
| --- |
| **Note: this document contains sensitive configuration data and must be kept secure at all times, especially when printed** |

**07/10/2020**

**Document Control**

This document is controlled and maintained according to the documentation standards and procedures of Nottingham City Council. All requests for changes to the document should be sent to the authors. Any new issues will be sent to the recipients as defined within the distribution list maintained by the authors. Requests for additional copies of this document should be sent to the author to ensure that alterations or amendments to the distribution list are properly controlled.

**Copyright rests with:** Nottingham City Council.

Loxley House

Station Street

Nottingham

ENGLAND

NG2 3NG

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Description** | **Editor** | **Date** |
| 1.0 | Create documentation | Stuart Chaffin | 21/07/2020 |
| 1.1 | Expanded on questions and formatting changes | Stuart Chaffin | 05/08/2020 |
| 1.2 | Questionnaire further expanded and addition of a risk rating | Stuart Chaffin | 18/09/2020 |
| 1.3 | Added data categories section | Stuart Chaffin | 30/09/2020 |
|  |  |  |  |

**APPROVAL OF FINAL DOCUMENT**

These signatories confirm that this document has been internally reviewed.

|  |  |
| --- | --- |
| **Name** | **Signature / Date** |
|  |  |
|  |  |

**Distribution (if different from Approvers):**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title** | **Date of Issue** | **Version** |
|  |  |  |  |
|  |  |  |  |

# Requester Details

|  |  |  |  |
| --- | --- | --- | --- |
| **Requester Name** |  | **Request Date** |  |
| **Contact No.** |  | | |
| **Reference No.**  (IT Service Desk Call Ref) |  | | |
| **DPIA Reference**  (DPIA Ref if applicable) |  | | |

Once the questionnaire has been completed please attach it to your service request which can be raised via the [IT Self Service Portal](https://itservicedesk.nottinghamcity.gov.uk/).

# Product

Please provide detail about the system, this should include the product(s) name, and an overview of the service(s) provided and the information used, shared or stored:

|  |
| --- |
|  |

# Manufacturer

Please provide detail about the system manufacturer, this should include the company name and address, telephone number and website. (If possible also include a contact for any queries arising from this assessment):

|  |
| --- |
|  |

# Accreditations and testing

Is the provider able to demonstrate that they are accredited to any standards, for example any of the following accreditations?

ISO 27001 / CSA STAR

PCI-DSS

Cyber Essentials Plus

PSN

SOC 2 type 2 report

HSCN

Other

Please evidence this below, attach relevant certification information to the response:

|  |
| --- |
|  |

Please provide information regarding any internal and external security testing performed by the supplier company, including vulnerability assessments and penetration testing. (This should include the timeframes that these activities are undertaken and how outcomes are remediated).

|  |
| --- |
|  |

# Hosting

Where will the system be located / hosted?

On-premise Installation (System installed / located within the Council’s network)

Hosted solution (Hosted by a 3rd party, this includes Cloud services)

Hybrid (Contains elements of both a Hosted solution and On-premise installation)

Please provide further information about the infrastructure:

|  |
| --- |
|  |

# Access

Which best describes the network access model for the system:

Public, accessible over the internet by anyone that knows the address

This includes Cloud and On-premise systems that are presented out to the internet in an unrestricted manner

IP Restriction, access restricted to a defined list of networks

Restricted, accessible only from the Corporate network

On-premise installations that are not presented out to the internet

Site to site VPN, secure connection established between Organisations

Other

Please provide further information, detailing any restrictions or safeguards:

|  |
| --- |
|  |

Which methods of access are available for users of the system:

Web Application - Standard

Accessed via a Browser (IE, Edge, Chrome) with no special requirements

Web Application - Additional Requirements

Web Applications that require additional Software or Plugins to enable full functionality

Desktop Application

Application that runs locally on a computer device

Mobile Application

Applications that run on Smartphones or Tablets

Other

Please provide further information:

|  |
| --- |
|  |

# Administration

Which role/post within the Local Authority is responsible for **configuring and** **administering the system**, to ensure the system is appropriately secured, updated and supported?

|  |
| --- |
|  |

Which role/post within the Local Authority is responsible for **user administration** within the system, adding, removing and managing users to ensure that only the correct people have the correct access, and leavers are effectively removed?

|  |
| --- |
|  |

Is any administration provided by a 3rd party?

Yes

No

If so, please provide further information:

|  |
| --- |
|  |

If any administration is provided by a 3rd party, does the organisation undertake personnel screening of all staff in line with the [Baseline Personnel Security Standard](https://www.gov.uk/government/publications/government-baseline-personnel-security-standard) (BPSS) or equivalent process?

Yes

No

N/A

Please provide further information to evidence this, or detail equivalent processes:

|  |
| --- |
|  |

# Authentication

Will the system make use of Single Sign On? (Be integrated with the Council’s Active Directory, allowing users to login with the same domain credentials).

Yes, Single Sign On will be used

No, the system will utilise a separate database of Users

Please provide further information about the password policy and its enforcement (length, age, complexity, lockout etc…)

|  |
| --- |
|  |

Does the system support Multi-factor authentication?

Yes

No

If Yes, will the system be configured to enforce the use of Multi-factor authentication for all users?

Yes

No

N/A

Please provide further information regarding the MFA implementation, or justify why it is not required:

|  |
| --- |
|  |

# Processing and storage of data and backups

Is all data, including live systems, backups and replication to any other sites for resilience or customer service operations stored and processed within the European Economic Area? (This includes access through or from VPN's, thin client services, customer service operations and system administration).

Yes

No

If any processing or storage of data is subcontracted to any 3rd parties, is the storage and use of data and systems within the European Economic Area; this includes the use of data within applications?

Yes

No

N/A

Are all system administration and support staff located within the European Economic Area (EEA)?

Yes

No

Please provide further information to evidence this, or what other controls are in place if this is not the case, reference any contacts or agreements where this is detailed:

|  |
| --- |
|  |

# Data categories

Identify the categories of data that will be processed by the system, select all that apply.

Public Data

Information that’s freely available to all employees or external entities.

Financial Data

Data containing financial information e.g. account balances and history, budgets, invoices, statements, assets and valuations

Personal Data

GDPR defines [personal data](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/) as information relating to natural persons who:

* can be identified or who are identifiable, directly from the information in question; or
* who can be indirectly identified from that information in combination with other information.

Note: This includes user management, where individuals are identified in order to provide access to the system.

Special Category Data

GDPR defines [special category data](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data) as:

* personal data revealing racial or ethnic origin;
* personal data revealing political opinions;
* personal data revealing religious or philosophical beliefs;
* personal data revealing trade union membership;
* genetic data;
* biometric data (where used for identification purposes);
* data concerning health;
* data concerning a person’s sex life; and
* data concerning a person’s sexual orientation.

Other

Any other non-personal sensitive information which is controlled by the company and needs to be protected.

Please provide further information, commenting on the sensitivity of the data stored within the system:

|  |
| --- |
|  |

# Data in transit

Is all application data, including customer data in transit encrypted using at least TLS v1.2 or IPSEC when transmitted or presented onto public or shared networks (including traffic exchanged over HTTPS, VPNs, APIs or other network-based technologies)?

Yes

No

Please provide further information to evidence this, reference any official system / specification documentation where this is detailed:

|  |
| --- |
|  |

# Data at rest

Is all customer data at rest encrypted using AES 128 bit or AES 256 bit encryption (including backups, virtual machines and databases)?

Yes

No

Please provide further information to evidence this, or what other controls are in place if this is not the case:

|  |
| --- |
|  |

# System and data architectures

To help with the assessment please include documentation of the planned implementation architectures showing systems and network devices. (If a data architecture is available please include this too).

|  |
| --- |
|  |

# Supporting documents

Please attach any other available supporting documents pertaining to the system, these can include the service provider contract, service level agreement, data processing agreement, product documentation, user documentation etc…:

|  |
| --- |
|  |

## IT Security to complete

This section is to be completed by an IT Security Analyst once the questionnaire has been completed.

|  |  |
| --- | --- |
| **Reviewed By** |  |
| **Completion Date** |  |

Rate the overall IT Security risk associated with the system, based on the information provided and safeguards in place as detailed in this document, and provide a recommendation, or not, for sign off:

Low Risk - Recommended for Sign Off

Little to no IT Security concerns with the system and / or its implementation

Medium Risk - Recommended for Sign Off

Some areas of IT Security concern with the system and / or its implementation, but these are tolerable

High Risk - NOT Recommended for Sign Off

Serious IT Security concerns with the system and / or its implementation

Provide comment on the overall IT Security of the system as detailed, highlighting any concerns or recommendations:

|  |
| --- |
|  |