NCC-042748-19 Information and Cyber Security Risks

Dear Requester,

Further to your request for information under the freedom of information act, please see below in response.

Dear Sir,
Freedom of Information Request – Information and Cyber Security Risk Management.

This is a request under the Freedom of Information Act 2000 and relates to how your organisation undertakes information and cyber security risk assessments.
Please could you tell me:

1. Does your organisation have a formal policy regarding the production of information and or cyber security risk assessments? **Yes.**
   a. If yes, please can you provide a copy of the above policy? **Information Security Policy and Risk Standard and Procedure is enclosed**

2. Does your organisation hold a register of Information and/or cyber security risk (outside that of the corporate risk register), and if yes:
   a. **yes**
   b. Please can you list the top ten Information and/or Cyber Security Risks? **Exempt from disclosure – Under s.33 of the Freedom of information act**

3. How many risks are there in total on the register? **25**
c. Please state how many risks would be categorised as the highest risk level (i.e. Critical)? **7**
d. Please state how many risks would be categorised as the second highest risk level (i.e. Critical)? **11**
e. Please state how many risks would be categorised as the third highest risk level (i.e. Critical)? **3**
f. How many risk levels do you have in total (i.e. 5)? **4**

4. Do any of the identified information and or cyber security risks also exist on the corporate risk register? **No**
   a. If yes, what are those risks? **n/a**

5. When undertaking an information / cyber security risk assessment, does the authority follow a structured risk assessment process? **Yes**
   a. If so, what is that process? **See process in 1a**

6. Does your orgnisation follow ISO31000 when undertaking an information / cyber security risk assessment? **No**

7. Does your orgnisation hold ISO27000 accreditation ? **No**

8. Does your organisation have a policy of adhering to any information security standard or framework (i.e. ISO27000, NIST etc)? **Yes - Cyber Essentials and PSN**

a. If yes, please provide a copy of the above policy? **For Cyber Essentials please see : https://www.gov.uk/government/publications/cyber-essentials-scheme-overview for PSN please see : https://www.gov.uk/government/groups/public-services-network**

9. Does the authority have the following roles within the origination:
a. Chief Security Officer (CSO), - **NO**
i. If yes, which role does the CSO report into?
b. Chief Information Security Officer (CISO) - **NO**
i. If yes, which role does the CISO report into?
c. Head of Information Security (Hd InfoSec) - **NO**
i. If yes, which role does the Hd InfoSec report into?

10. Who within your organisation who is accountable for undertaking information / cyber security risk assessments (i.e. Chief Information Security Officer, Head of Information Security, Head of Information Technology) ? **Head of ICT, Operational Delivery Management Team and Risk Manager, Security Architect**

11. Who within the authority is responsible for undertaking information / cyber security risk assessments (i.e. Chief Information Security Officer, Head of Information Security, Head of Information Technology) ? **Head of ICT, Operational Delivery Management Team and Risk Manager**

12. How many people within the organisation are responsible for undertaking information / cyber security risk assessments? **6 in ICT, 5 in Information Governance, 8 in Emergency Planning = 19.**

13. Does the person(s) responsible for undertaking information / cyber security risk assessment:
a. Have any formal training in this regard? **Yes**
i. If so, what was it? **Management of Risk – M_o_R**
b. Have any industry qualifications/certification in this regard?
i. If so, what are they? **See above**

14. How many people (permanent and contractors) currently work for the authority? **Approx 7500**

15. How many people (permanent and contractors) currently work for the authority in information technology roles? **Approx. 421**

16. How many people (permanent and contractors) currently work for the authority in information / cyber security roles? **8 in ICT, 5 in Information Governance**

We trust this now resolves your enquiry, however should you have any further queries please do not hesitate to contact me directly on the details below.

We suggest all requesters search under our publication scheme in advance of requesting information under the freedom of information act.

Nottinghamshire County Council regularly publishes previous FOIR, s and answers on its website, under Disclosure logs. (see link) http://site.nottinghamshire.gov.uk/thecouncil/democracy/freedom-of-information/disclosure-log/

You can use the search facility using keywords. i.e. un regulated / care / home etc.

If you are unhappy with the service you have received in relation to your request and wish to make a complaint or request a review of our decision, you should write to the Team Manager, Complaints and Information Team, County Hall, West Bridgford, Nottingham, NG2 7QP or email complaints@nottscc.gov.uk .

Kind Regards

Complaints and Information Team
Nottinghamshire County Council
County Hall