Request Reference: FOI/013/24
Published: 01 July 2024

Information requested:

Please can the below FOI request kindly be responded to in excel format

LAN
a1 Which primary LAN hardware do you use (eg Extreme, Juniper, Cisco)
a2 When did you last conduct a major refresh of this infrastructure/how many devices?
a3 Who is the reseller or supplier of this LAN hardware?
a4 Who maintains the LAN?
a5 When is your maintainance renewal/expiry date ?
a6 Have you recently reviewed/when are you next reviewing this infrastructure?

WLAN Wireless LAN
b1 Which primary WLAN hardware do you use (eg Extreme, Juniper, Cisco)
b2 When did you last conduct a major refresh of this infrastructure/how many devices?
b3 Who is the reseller or supplier of this WLAN hardware?
b4 Who maintains the WLAN?
b5 When is your maintainance renewal/expiry date ?
b6 Have you recently reviewed/when are you next reviewing this infrastructure?

Data Centre
c1 Which primary data centre hardware do you use (eg Extreme, Juniper, Cisco)
c2 When did you last conduct a major refresh of this infrastructure/how many devices?
c3 Who is the reseller or supplier of this data centre hardware?
c4 Who maintains the data centre equipment?
c5 When is your contract renewal/expiry date ?
c6 Have you recently reviewed/when are you next reviewing this infrastructure?
c7 Which DC compute technology do you use? (eg HP, Lenovo, Supermicro)
c8 Which DC storage technology do you use? (eg netapp, dell, IBM)

WAN/Internet Connectivity
d1 Who provides your WAN (eg BT, Virgin)
d2 Who provides your internet connectivity (eg BT, Virgin)
d3 When is your maintainance renewal/expiry date ?
d4 Who provides your SD-WAN (eg Palo Alto, Meraki)
d5 Do you plan to introduce SD-WAN in the future?
d6 Have you recently reviewed/when are you next reviewing this infrastructure?
d7 Which hypervisor do you use (eg VMware)

SIP
e1 Which SIP carrier do you use (eg BT, Gamma, Virgin)
e2 Who provides/resells this SIP?
e2 How many SIP channels do you have
e3 When is your contract renewal/expiry date ?
e4 Have you recently reviewed/when are you next reviewing this service?

Mobile
f1 Which Mobile carrier do you use (eg Vodafone)
f2 Who provides/resells this service ?
f2 How many mobile connections do you have
f3 When is your contract renewal/expiry date ?
f4 Have you recently reviewed/when are you next reviewing this service?

Telephony
g1Which phone systems do you use (eg Mitel, Avaya, 8x8)
g2 When was the current system installed?

g3 Is this on premise or cloud based?
g4 How many users?
g5 When is your contract renewal/expiry date ?
g6 Have you recently reviewed/when are you next reviewing this service?

Teams Phone System
h1 Do you use Microsoft for PSTN calling?
h2 Which types of Microsoft telephony do you use (eg Calling plan, Skype, Operator Connect, Direct routing)
h3 How many users?
h4 If you dont currently use, are you looking to implement ?
h5 Have you recently reviewed/when are you next reviewing this service?

Contact centre
i1 Which contact centre systems do you use (eg Genesys, Avaya, Enghouse)
i2 When was the current system installed?
i3 Is this on premise or cloud based?
i4 How many agents?
i5 When is your contract renewal/expiry date ?
i6 Have you recently reviewed/when are you next reviewing this service?

Response:

We have provided a spreadsheet with the information requested.

Advice and Guidance

We have withheld some information under the following exemptions;

1. FOISA section 30(c) as disclosure would be likely to substantially prejudice the effective contact of public affairs. This is because disclosure of detailed information about our infrastructure and systems could be used to identify vulnerabilities that could be exploited to disrupt the organisation's digital systems and platforms.

2. FOISA section 35(1)(f) and 2(i) as disclosure would substantially prejudice the maintenance of security and good order in prisons or in other institutions where persons are lawfully detained for the purpose to secure the health, safety and welfare of persons at work because disclosure of detailed information about our infrastructure and systems could be used to be used to identify vulnerabilities that could be exploited to disrupt the organisation's digital systems and platforms. Such a disruption would affect access to patient management plans and risk assessments of individuals with a propensity for violence and thus increase the risks of assaults against staff.

3. FOISA section 35(1)(f) and 2(j) as disclosure would substantially prejudice the maintenance of security and good order in prisons or in other institutions where persons are lawfully detained for the purpose to protect persons, other than persons at work, against risk to the health and safety where that risk arises out of, or in connection with, the actions of persons at work because disclosure of detailed information about our infrastructure and systems could be used to be used to identify vulnerabilities that could be exploited to disrupt the organisation's digital systems and platforms. Such a disruption would affect access to patient management plans and risk assessments of individuals with a propensity for violence and thus increase the risks of assaults against visitors or other patients.

4. FOISA section 39(1) as disclosure would be likely to endanger the physical or mental health or safety of an individual because disclosure of detailed information about our infrastructure and systems could be used to be used to identify vulnerabilities that could be exploited to disrupt the organisation's digital systems and platforms. Such a disruption would affect access to patient health records and prescribing information. This would disrupt the day to day operation of a ward which in turn may affect the mental health of our patients. A deterioration of our patients' mental health is often associated with an increase in violent behaviour which places patients, staff and visitors at an increased risk of assault.

As required, we undertook a public interest test before we apply these exemptions, in which we concluded that the public interest was best served by the effective operation of the State Hospital and that disclosure would make public information that could be used to disrupt that operation. Such a disruption would impact the health and safety of staff, patients, visitors and the public. Patients' mental and physical health would also be affected by disruption to healthcare systems. The organisation is subject to NIS audits which provides independent scrutiny of our digital infrastructure.