St Helens and Knowsley Teaching Hospitals NHS Trust

Ref no:	695030317
From:	Public
Date:	03/03/17
Subject:	IT Services

REQUEST

I am writing to make an open government request for all the information to which I am entitled under the Freedom of Information Act 2000.

Please send me information with regard to the following:

- Number of employees **- 6000 at St Helens& Knowsley Trust**
- URL Filtering vendor – **See response below**
- URL Filtering annual cost – **See response below**

- URL Filtering expiry date – **See response below**
- Firewall vendor – **See response below**
- Firewall annual cost – **See response below**
- Firewall expiry date – **See response below**
- Sandboxing vendor – **See response below**
- Sandboxing annual cost – **See response below**
- Sandboxing expiry date – **See response below**
- Guest WiFi vendor – **See response below**
- Guest WiFi annual cost – **See response below**
- Guest WiFi expiry date – **See response below**

· Number of Egress Points **– See response below**

· VPN Vendor **– See response below**

· Number of IT Security Breaches in past 12 months - **One**

· Are you using Office 365 – **No**

· Are you scanning SSL traffic **– See response below**

· What are your MPLS costs per year **– See response below**

· How many locations do you have connected to your MPLS Network – **See response below**

· Who are the people responsible for Network Security – **SIRO / Christine Walters**

· Which cloud Platform or platforms as a Service (PAAS) are you using / looking to use. (AWS, Azure, Google): **N/A**

· Who is your Head of Security or Chief Information Security Officer: **SIRO / Christine Walters**

· Who is your Chief Information Officer or Chief Technology Officer: **Rowan Pritchard Jones**

· Who is your Senior Cloud Architect: **N/A**

· What VPN / RAS solution do you use– **See response below?**

· How much is your VPN / RAS solution renewal cost – **See response below?**

· When is your VPN / RAS solution due to be renewed? – **See response below**

RESPONSE

General Response as below:

The Trust must do its utmost to protect patient and staff information.

Patient information and staff information are the foundations upon which healthcare is built, and the Trust have a clear responsibility to safeguard this information to ensure we are able to provide the necessary care to our service users.

To provide the requested information above would highlight any vulnerability, should any such vulnerability exist (within hardware or software or architecture or Vendor, etc.), within our IT infrastructure which could be exploited for the purposes of ransomware, other malware, or to withhold/disrupt IT functionality within the Trust. Therefore, to confirm or deny such architecture in our IT network is likely to assist criminal offenders thereby seriously threatening the effective delivery of healthcare by the Trust. The act of gathering information as requested, in the hacking arena is known as foot-printing and our network architecture is closely protected to at least NHS protect if not NHS Confidential. Therefore:

To confirm or deny what Standard Firewall (Network) or SSL scanning - service(s) protects our corporate Network from unauthorised access and other Internet security threats may motivate attacks against our network which would massively hinder our abilities to safeguard the service user healthcare information and staff information that we require to coordinate our services.

To confirm the infrastructure DMZ, IDS, Honey Pots or Anti-Virus (sandboxing), etc. hardware & software could expose vulnerabilities within one or more of our IT infra-structures which could subsequently lead to attacks, data loss, and loss of public confidence.

To confirm the infrastructure VPN/RAS, etc. hardware & software could expose vulnerabilities within one or more of our IT infra-structures which could subsequently lead to attacks, data loss, and loss of public confidence.

To confirm the infrastructure Guest WiFi, etc. hardware & software could expose vulnerabilities within one or more of our IT infra-structures which could subsequently lead to attacks, data loss, and loss of public confidence.

Our patients (and staff) must have confidence that their very sensitive personal data will be held securely.

Again, providing information about what contracts/suppliers/vendors could also expose what applications we use (including cloud based services) and aid to the foot printing phenomena.

They (patients & staff) must have confidence that we'll be able to provide the services they need.

Therefore, providing the specific requested information would put their confidence at risk.

Furthermore, loss of patient and staff data by such an attack would massively impact upon our ability to provide effective healthcare to our service users.

And therefore, this would be extremely harmful to the public & the services the Trust provides.