

Date: 31/10/2016

FREEDOM OF INFORMATION REQUEST 013073 – Cyber security

1. Standard Firewall (Network) - Firewall service protects your corporate Network from unauthorised access and other Internet security threats
2. Intrusion Detection - network intrusion detections systems (IDS) and network intrusion prevention systems (IPS) services that detect Web application attacks and include anomaly-awareness in addition to handling older threats that haven't disappeared.
3. Web Applications Firewall - A Web application firewall (WAF) is a firewall that monitors, filters or blocks the HTTP traffic to and from a Web application.
4. Threat Monitoring - organizations and security analysts to identify and protect against security threats.
5. Anti-virus Software Application - Anti-virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.
6. Encryption Facilities - s a host based software solution designed to encrypt sensitive data before transferring it to tape for archival purposes or business partner exchange.

For each of the different types of cyber security services can you please provide me with:

1. Who is the existing supplier for this contract? Exemption (43)
2. What does the organisation spend for each of contract? Inhouse therefore not Applicable
3. What is the description of the services provided for each contract? Inhouse therefore not Applicable
4. What is the expiry date of each contract? Inhouse therefore not Applicable
5. What is the start date of each contract? Inhouse therefore not Applicable
6. What is the contract duration of contract? Inhouse therefore not Applicable
7. What is the hardware brand? If available. ? Exemption (43)
8. What is the software brand? If available? ? Exemption (43)
9. The responsible contract officer? Full name, job title, contact number and direct email address. CIO Mark Stanton. www.terafirma.nhs.uk

*Exemption (43) has been applied given it is commercially sensitive in that providing the information may compromise information security. Therefore it is not in the public interest to provide.