ICT security

Reference No: 033/2017
Request Date: 28/03/2017

Request

1. Has your department been a victim of Ransomware?
2. If Yes - did you pay to release your data?
3. If yes, How much did you pay?
4. If no, how did you gain back control of your data?
5. Do you have the following in place:
    a. Backup – if yes
        I. What software do you use?
        II. When does your maintenance expire?
        III. How many TB of Data do you back up?
    b. Firewall – if yes:
        I. What firewall do you use?
        II. When does maintenance expire?
6. What Email system do you use, how many users?
7. Are you planning to migrate to Microsoft Office 365?
    a. If yes, why
    b. Will you be adding extra security to this?
8. What email security solution do you use?
9. Do you use a public cloud provider, if so which one?
    a. How do you secure the data in the cloud?

Response

1. No
2. N/A
3. N/A
4. N/A

5. Please note that we are not able to provide the information you have requested in relation to our IT Backup and Firewall systems under Section 31 Law Enforcement – S31(1)(a) disclosure would be likely to prejudice prevention or detection of crime.
   We are applying this exemption to protect our Service and the wider community from potential crime and its consequences and to prevent the publishing of such information falling into the hands of those with malicious intent.
   We have a duty as an Emergency Service to ensure that our systems are protected and by releasing such information into the public domain we consider would compromise our ability to carry out that duty.
   We consider that it is in the interest of the majority of the public to protect our IT systems to allow us to carry out our duty to ensure public safety and conclude that the detail of this information is not necessary to meet the public interest and therefore confirm our decision that the public interest is better served by not disclosing this detailed information

6. Outlook

7. No

   a. N/A

   b. N/A

8. Sophos

9. No

   a. N/A