7 March 2015

Our Ref: IM-FOI-2015-0073

Sir Stephen House QPM
Chief Constable

FOI Central Processing Unit
173 Pitt Street
Glasgow
G2 4JS

foi@scotland.pnn.police.uk

FREEDOM OF INFORMATION (SCOTLAND) ACT 2002
SUBJECT: Servers, backup software and other storage

I refer to your email dated 2015, regarding the above which has been handled in accordance with the Freedom of Information (Scotland) Act 2002 (FOISA). Please accept my apologies for the delay in replying.

I have repeated your request below for ease of reference.

1. How many Servers (Hosts) do you currently have and what % of these are virtualised?

We have approximately 3000 Servers of which 75% are virtualised.

2. Which Hypervisor are you using for your virtual estate? VMWare/HyperV/Others?

3. Which manufacturer provides your primary storage?

4. What visibility/planning/monitoring tools do you currently use within your virtual environment

Unfortunately, I am unable to provide the information requested above as this information is considered to be exempt in terms of the Freedom of Information

(Scotland) Act 2002 (the Act). Section 16 of the Act requires Police Scotland to provide you with a notice which: (a) states that it holds the information, (b) states that it is claiming an exemption, (c) specifies the exemption in question and (d) states, if that would not be otherwise apparent, why the exemption applies. Where information is considered to be exempt, this letter serves as a Refusal Notice that information is held and an explanation of the appropriate exemption is provided.

Section 35 (1) (a) & (b) – Law Enforcement

To disclose information which has the potential to compromise Police Scotland's IT security could undermine policing and jeopardise national security. If police forces lose control of their IT systems, crime recording databases will be inaccessible as well as software which is used by departments such as control room. If the Police force is unable to operate its functions and provide an equivalent service, those with the inclination to do so, will take advantage of the Police force's vulnerability and increase criminal activities which then place the general public at risk and a fear of crime is realised.

The cumulative effect of providing all of the requested information to you, could mean those individuals intent on criminality gathering information from the public domain which would undoubtedly have even more impact when linked to other information gathered from various sources about police systems. The more information disclosed over time will give a more detailed account of the information infrastructure of not only a divisional area, but also the country as a whole.

Furthermore, to disclose information regarding the architecture, control and infrastructure of a police force's IT systems could possibly make them vulnerable to hacking. We cannot predict how disclosed information will be used by individuals but if this a possibility, not only personal information but also investigative information could be accessed, breaching data protection laws and jeopardising the safety of individuals as well as any on-going investigations.

Factors favouring disclosure

To disclose the information would demonstrate that the Police force is being open and transparent and it will allow the public to see where public funds are spent.

Factors favouring non-disclosure

To disclose the information will undermine policing and jeopardise national security. Individuals will gain knowledge about the Police Scotland's IT systems which would leave the Police force vulnerable to IT attacks and 'hacking' which have the potential to disrupt police functions, hinder the prevention and detection of crime and place the general public at risk of an increase in criminal activity.

Balance Test

The police will not disclose information which could place the public at risk or undermine their capabilities in carrying out their core function of preventing and detecting crime. Although there is a public interest in openness and transparency, there is a greater interest in protecting the public from harm. Therefore, it is our opinion that the balance lies with non-disclosure of the information.

4. What software are you current using for your backup solution?

For the reasons already detailed above, we consider this information exempt from disclosure for law enforcement reasons.

i. Who provides this?

SCC

ii. When is the maintenance due for renewal?

Renewed annually and due 31st March 2015

I trust that the information available is of assistance and should you require any further assistance concerning this matter please contact me on (01224) 305740 quoting the reference number given.

If you are not satisfied with the way in which your request has been dealt with, you are entitled in the first instance and within 40 working days of receiving this letter to request a review of the decision made by the Service. Should you wish to do so, contact details are; Police Scotland, FOI Central Processing Unit, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH. (Or email foi@scotland.pnn.police.uk).

Once informed of the review decision, if you are still not satisfied, then you are entitled to apply to the Scottish Information Commissioner within six months for a decision. The contact details are: Office of the Scottish Information Commissioner, Kinburn Castle, Doubledykes Road, St Andrews, Fife, KY16 9DS, telephone 01334 464610. Should you wish to appeal against the Scottish Information Commissioner's decision, there is an appeal to the Court of Session on a point of law only.

Yours sincerely,

Mr Nicky Leiper
Information Management
Police Scotland