



## FREEDOM OF INFORMATION

FOI REFERENCE: 083/21 DATE RECEIVED: 31 August 21

**REQUEST** 

I am writing to you under the Freedom of Information Act 2000 to request the following information from Staffordshire Fire and Rescue Service. Please can you answer the following questions:

1. In the past three years has your organisation:

- a. Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?)
  - i. If yes, how many?
- b. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)
- c. Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)
- d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?
  - i. If yes was the decryption successful, with all files recovered?
- e. Used a free decryption key or tool (e.g. from <a href="https://www.nomoreransom.org/">https://www.nomoreransom.org/</a>)?
  - i. If yes was the decryption successful, with all files recovered?
- f. Had a formal policy on ransomware payment?
  - i. If yes please provide, or link, to all versions relevant to the 3 year period.
- g. Held meetings where policy on paying ransomware was discussed?
- h. Paid consultancy fees for malware, ransomware, or system intrusion investigation
  - i. If yes at what cost in each year?
- i. Used existing support contracts for malware, ransomware, or system intrusion investigation?
- j. Requested central government support for malware, ransomware, or system intrusion investigation?
- k. Paid for data recovery services?
  - i. If yes at what cost in each year?
- I. Used existing contracts for data recovery services?
- m. Replaced IT infrastructure such as servers that have been compromised by malware?
  - i. If yes at what cost in each year?
- n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?
  - i. If yes at what cost in each year?
- o. Lost data due to portable electronic devices being mislaid, lost or destroyed?
  - i. If yes how many incidents in each year?
- 2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?
  - a. If yes is this system's data independently backed up, separately from that platform's own tools?

FOI Reference Number:

Issue Date:

Page 1 of 4

Any printed documents are considered uncontrolled.

Official







- 3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)
  - a. Mobile devices such as phones and tablet computers
  - b. Desktop and laptop computers
  - c. Virtual desktops
  - d. Servers on premise
  - e. Co-located or hosted servers
  - f. Cloud hosted servers
  - g. Virtual machines
  - h. Data in SaaS applications
  - i. ERP / finance system
  - j. We do not use any offsite back-up systems
- 4. Are the services in question 3 backed up by a single system or are multiple systems used?
- 5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?
- 6. How many Software as a Services (SaaS) applications are in place within your organisation?
  - a. How many have been adopted since January 2020?

## **RESPONSE**

- 1. In the past three years has your organisation:
  - a. Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?)
    - i. If yes, how many?
  - b. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)
  - c. Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)
  - d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?
    - i. If yes was the decryption successful, with all files recovered?
  - e. Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)?

No

FOI Reference Number:

Issue Date:

Page 2 of 4

Any printed documents are considered uncontrolled. You must checkwith the current version on Staffnet.





| f. Had a formal policy on ransomware payment?  i. If yes please provide, or link, to all versions relevant to the 3 year period. g. Held meetings where policy on paying ransomware was discussed? Yes h. Paid consultancy fees for malware, ransomware, or system intrusion investigation No i. If yes at what cost in each year? i. Used existing support contracts for malware, ransomware, or system intrusion investigation? No j. Requested central government support for malware, ransomware, or system intrusion investigation? No k. Paid for data recovery services? No i. If yes at what cost in each year? l. Used existing contracts for data recovery services? No m. Replaced IT infrastructure such as servers that have been compromised by malware? No i. If yes at what cost in each year? n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware? No i. If yes at what cost in each year? o. Lost data due to portable electronic devices being mislaid, lost or destroyed? No i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerty G Suite) or Microsoft's Office 365? Not fully implemented yet a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.) a. Mobile devices such as phones and tablet computers b. Desktop and laptop computers Yes c. Virtual desktops Yes d. Servers on premise Yes c. Virtual machines Yes h. Data in SaaS applications NA   |         |  |
|---|---------|--|
| i. If yes please provide, or link, to all versions relevant to the 3 year period. g. Held meetings where policy on paying ransomware was discussed? Yes h. Paid consultancy fees for malware, ransomware, or system intrusion investigation No i. If yes at what cost in each year? i. Used existing support contracts for malware, ransomware, or system intrusion investigation? No j. Requested central government support for malware, ransomware, or system intrusion investigation? No k. Paid for data recovery services? No i. If yes at what cost in each year? l. Used existing contracts for data recovery services? No m. Replaced IT infrastructure such as servers that have been compromised by malware? No i. If yes at what cost in each year? n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware? i. If yes at what cost in each year? o. Lost data due to portable electronic devices being mislaid, lost or destroyed? No i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365? Not fully implemented yet a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.) a. Mobile devices such as phones and tablet computers b. Desktop and laptop computers Yes c. Virtual desktops Yes d. Servers on premise Yes c. Co-located or hosted servers N/A g. Virtual machines Yes h. Data in SaaS applications  |         | <ul> <li>i. If yes was the decryption successful, with all files recovered?</li> </ul>       |
| g. Held meetings where policy on paying ransomware was discussed?  h. Paid consultancy fees for malware, ransomware, or system intrusion investigation No  i. If yes at what cost in each year? i. Used existing support contracts for malware, ransomware, or system intrusion investigation?  No  j. Requested central government support for malware, ransomware, or system intrusion investigation?  No  k. Paid for data recovery services?  l. Used existing contracts for data recovery services?  n. Replaced IT infrastructure such as servers that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes at what cost in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers  Yes  c. Virtual desktops  Yes  d. Servers on premise  Yes  Co-located or hosted servers  NA  JUITUAL Machines  Yes  h. Data in SaaS applications   | f.      |  |
| discussed?  Neal donsultancy fees for malware, ransomware, or system intrusion investigation  No  i. If yes at what cost in each year?  i. Used existing support contracts for malware, ransomware, or system intrusion investigation?  No  j. Requested central government support for malware, ransomware, or system intrusion investigation?  No  k. Paid for data recovery services?  No  i. If yes at what cost in each year?  l. Used existing contracts for data recovery services?  M. Replaced IT infrastructure such as servers that have been compromised by malware?  No  i. If yes at what cost in each year?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  No  i. If yes at what cost in each year?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  Yes  b. Desktop and laptop computers Yes  c. Virtual desktops  Yes  d. Servers on premise  Yes  Co-located or hosted servers  NA  g. Virtual machines  NA  yirtual machines  NA  Virtual machines  NA  Virtual machines  NA   |         |  |
| h. Paid consultancy fees for malware, ransomware, or system intrusion investigation  No  i. If yes at what cost in each year?  i. Used existing support contracts for malware, ransomware, or system intrusion investigation?  No  j. Requested central government support for malware, ransomware, or system intrusion investigation?  No  k. Paid for data recovery services?  No  i. If yes at what cost in each year?  l. Used existing contracts for data recovery services?  No  m. Replaced IT infrastructure such as servers that have been compromised by malware?  No  i. If yes at what cost in each year?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. If yes at what cost in each year?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes  c. Virtual desktops  Yes  d. Servers on premise  Yes  d. Cloud hosted servers  NA  g. Virtual machines  Yes  h. Data in SaaS applications  NA         | g.      |  |
| investigation No i. If yes at what cost in each year? i. Used existing support contracts for malware, ransomware, or system intrusion investigation? No j. Requested central government support for malware, ransomware, or system intrusion investigation? No k. Paid for data recovery services? No i. If yes at what cost in each year? l. Used existing contracts for data recovery services? No m. Replaced IT infrastructure such as servers that have been compromised by malware? No i. If yes at what cost in each year? n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware? No i. If yes at what cost in each year? o. Lost data due to portable electronic devices being mislaid, lost or destroyed? No i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365? Not fully implemented yet a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.) a. Mobile devices such as phones and tablet computers b. Desktop and laptop computers Yes c. Virtual desktops Yes d. Servers on premise Yes e. Co-located or hosted servers NA g. Virtual machines Yes h. Data in SaaS applications NA   |         |  |
| i. If yes at what cost in each year?  i. Used existing support contracts for malware, ransomware, or system intrusion investigation?  j. Requested central government support for malware, ransomware, or system intrusion investigation?  No  k. Paid for data recovery services?  i. If yes at what cost in each year?  l. Used existing contracts for data recovery services?  No  m. Replaced IT infrastructure such as servers that have been compromised by malware?  No  i. If yes at what cost in each year?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  No  i. If yes at what cost in each year?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes  c. Virtual desktops  Yes  d. Servers on premise  Yes  d. Servers on premise  Yes  Co-located or hosted servers  NA  g. Virtual machines  Yes  h. Data in SaaS applications   | h.      |  |
| <ul> <li>i. Used existing support contracts for malware, ransomware, or system intrusion investigation?  No  No  Requested central government support for malware, ransomware, or system intrusion investigation?  No  Relat for data recovery services?  No  i. If yes at what cost in each year?  I. Used existing contracts for data recovery services?  No  m. Replaced IT infrastructure such as servers that have been compromised by malware?  No  i. If yes at what cost in each year?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  No  i. If yes at what cost in each year?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes  c. Virtual desktops  Yes  d. Servers on premise  Yes  Servers on premise  Yes  Co-located or hosted servers  NA  G. Virtual machines  Yes  h. Data in SaaS applications  NA</li> </ul>   |         |  |
| investigation?  j. Requested central government support for malware, ransomware, or system intrusion investigation?  k. Paid for data recovery services?  l. Used existing contracts for data recovery services?  m. Replaced IT infrastructure such as servers that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. If yes at what cost in each year?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes  c. Virtual desktops  Yes  d. Servers on premise  Yes  Co-located or hosted servers  NA  y. Virtual machines  Yes  h. Data in SaaS applications  NA |         |  |
| j. Requested central government support for malware, ransomware, or system intrusion investigation?  k. Paid for data recovery services?  i. If yes at what cost in each year?  l. Used existing contracts for data recovery services?  No  m. Replaced IT infrastructure such as servers that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  i. If yes at what cost in each year?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes  c. Virtual desktops Yes  d. Servers on premise Yes  c. Co-located or hosted servers  NA  Joint and saaS applications  NA   | i.      |  |
| investigation?  k. Paid for data recovery services?  i. If yes at what cost in each year?  l. Used existing contracts for data recovery services?  m. Replaced IT infrastructure such as servers that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes c. Virtual desktops Yes d. Servers on premise Yes e. Co-located or hosted servers VA f. Cloud hosted servers VA y. Virtual machines Yes h. Data in SaaS applications VA  |         |  |
| k. Paid for data recovery services?  i. If yes at what cost in each year?  l. Used existing contracts for data recovery services?  m. Replaced IT infrastructure such as servers that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  yes  b. Desktop and laptop computers  Yes  d. Servers on premise  Yes  d. Servers on premise  Yes  c. Co-located or hosted servers  NA  Cloud hosted servers  NA  Virtual machines  Yes  h. Data in SaaS applications  | j.      |  |
| <ul> <li>i. If yes at what cost in each year?</li> <li>l. Used existing contracts for data recovery services? No</li> <li>m. Replaced IT infrastructure such as servers that have been compromised by malware? No <ul> <li>i. If yes at what cost in each year?</li> </ul> </li> <li>n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware? No <ul> <li>i. If yes at what cost in each year?</li> </ul> </li> <li>o. Lost data due to portable electronic devices being mislaid, lost or destroyed? No <ul> <li>i. If yes how many incidents in each year?</li> </ul> </li> <li>2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365? <ul> <li>Not fully implemented yet</li> <li>a. If yes is this system's data independently backed up, separately from that platform's own tools?</li> </ul> </li> <li>3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)</li> <li>a. Mobile devices such as phones and tablet computers <ul> <li>yes</li> <li>b. Desktop and laptop computers Yes</li> <li>c. Virtual desktops Yes</li> <li>d. Servers on premise Yes</li> <li>e. Co-located or hosted servers N/A</li> <li>g. Virtual machines Yes</li> <li>h. Data in SaaS applications N/A</li> </ul> </li> </ul>  |         |  |
| <ul> <li>I. Used existing contracts for data recovery services?  m. Replaced IT infrastructure such as servers that have been compromised by malware?  i. If yes at what cost in each year?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  i. If yes at what cost in each year?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?</li> <li>2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?</li> <li>3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes  c. Virtual desktops Yes  d. Servers on premise Yes  e. Co-located or hosted servers  NA  G. Virtual machines  Yes  h. Data in SaaS applications  NA</li> </ul>  | k.      |  |
| m. Replaced IT infrastructure such as servers that have been compromised by malware?  No  i. If yes at what cost in each year?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  No  i. If yes at what cost in each year?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes  c. Virtual desktops  Yes  d. Servers on premise  Yes  e. Co-located or hosted servers  N/A  g. Virtual machines  Yes  h. Data in SaaS applications  N/A  |         |  |
| i. If yes at what cost in each year?  n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  i. If yes at what cost in each year?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes  c. Virtual desktops  Yes  d. Servers on premise  Yes  e. Co-located or hosted servers  I. Cloud hosted servers  N/A  g. Virtual machines  Yes  h. Data in SaaS applications  N/A   |         |  |
| <ul> <li>i. If yes at what cost in each year?</li> <li>n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  <ul> <li>i. If yes at what cost in each year?</li> </ul> </li> <li>o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  <ul> <li>i. If yes how many incidents in each year?</li> </ul> </li> <li>2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  <ul> <li>a. If yes is this system's data independently backed up, separately from that platform's own tools?</li> </ul> </li> <li>3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  <ul> <li>a. Mobile devices such as phones and tablet computers</li> <li>yes</li> <li>b. Desktop and laptop computers</li> <li>Yes</li> <li>c. Virtual desktops</li> <li>Yes</li> <li>e. Co-located or hosted servers</li> <li>N/A</li> <li>g. Virtual machines</li> <li>Yes</li> <li>h. Data in SaaS applications</li> </ul> </li> </ul>   | m.      |  |
| n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?  i. If yes at what cost in each year?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes  c. Virtual desktops Yes  d. Servers on premise Yes  e. Co-located or hosted servers  NA  g. Virtual machines Yes  h. Data in SaaS applications  NA   |         |  |
| compromised by malware?  i. If yes at what cost in each year?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes  c. Virtual desktops Yes  d. Servers on premise Yes  e. Co-located or hosted servers  NA  f. Cloud hosted servers  NA  g. Virtual machines Yes  h. Data in SaaS applications  NA   |         |  |
| i. If yes at what cost in each year?  o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers  c. Virtual desktops  Yes  d. Servers on premise  Yes  e. Co-located or hosted servers  N/A  g. Virtual machines  Yes  h. Data in SaaS applications  N/A  | n.      |  |
| <ul> <li>o. Lost data due to portable electronic devices being mislaid, lost or destroyed?  No  i. If yes how many incidents in each year?</li> <li>2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?</li> <li>3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes  c. Virtual desktops  Yes  d. Servers on premise  Yes  e. Co-located or hosted servers  NA  g. Virtual machines  Yes  h. Data in SaaS applications</li> </ul>  |         |  |
| i. If yes how many incidents in each year?  2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?  Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers Yes c. Virtual desktops Yes d. Servers on premise Yes e. Co-located or hosted servers N/A g. Virtual machines Yes h. Data in SaaS applications N/A   |         |  |
| <ul> <li>i. If yes how many incidents in each year?</li> <li>2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365? Not fully implemented yet  <ul> <li>a. If yes is this system's data independently backed up, separately from that platform's own tools?</li> </ul> </li> <li>3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  <ul> <li>a. Mobile devices such as phones and tablet computers</li> <li>b. Desktop and laptop computers Yes</li> <li>c. Virtual desktops</li> <li>yes</li> <li>d. Servers on premise</li> <li>Yes</li> <li>e. Co-located or hosted servers</li> <li>N/A</li> <li>g. Virtual machines</li> <li>Yes</li> <li>h. Data in SaaS applications</li> </ul> </li> </ul>   | 0.      | ·  |
| <ol> <li>Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?         Not fully implemented yet         <ol> <li>If yes is this system's data independently backed up, separately from that platform's own tools?</li> </ol> </li> <li>Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)         <ol> <li>Mobile devices such as phones and tablet computers Yes</li> <li>Virtual desktops Yes</li> <li>Servers on premise Yes</li> <li>Co-located or hosted servers N/A</li> <li>Virtual machines Yes</li> <li>Data in SaaS applications</li> </ol> </li> </ol>   |         |  |
| <ul> <li>(Formerly G Suite) or Microsoft's Office 365? Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?</li> <li>3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers b. Desktop and laptop computers Yes c. Virtual desktops Yes d. Servers on premise Yes e. Co-located or hosted servers F. Cloud hosted servers N/A g. Virtual machines Yes h. Data in SaaS applications</li> </ul>  |         | i. If yes how many incidents in each year?   |
| <ul> <li>(Formerly G Suite) or Microsoft's Office 365? Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?</li> <li>3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers b. Desktop and laptop computers Yes c. Virtual desktops Yes d. Servers on premise Yes e. Co-located or hosted servers F. Cloud hosted servers N/A g. Virtual machines Yes h. Data in SaaS applications</li> </ul>  | 2 Doors | your organisation use a cloud based office suite system such as Google Workspace             |
| Not fully implemented yet  a. If yes is this system's data independently backed up, separately from that platform's own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers Yes  b. Desktop and laptop computers Yes  c. Virtual desktops Yes  d. Servers on premise Yes  e. Co-located or hosted servers N/A  f. Cloud hosted servers N/A  g. Virtual machines Yes  h. Data in SaaS applications N/A   |         |  |
| <ul> <li>a. If yes is this system's data independently backed up, separately from that platform's own tools?</li> <li>3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.) <ul> <li>a. Mobile devices such as phones and tablet computers</li> <li>b. Desktop and laptop computers</li> <li>c. Virtual desktops</li> <li>d. Servers on premise</li> <li>e. Co-located or hosted servers</li> <li>f. Cloud hosted servers</li> <li>h. Data in SaaS applications</li> </ul> </li> </ul>   | (F01111 |  |
| own tools?  3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers  b. Desktop and laptop computers  c. Virtual desktops  yes  d. Servers on premise  Yes  e. Co-located or hosted servers  MA  g. Virtual machines  Yes  h. Data in SaaS applications  NA   | 2       |  |
| <ul> <li>3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.) <ul> <li>a. Mobile devices such as phones and tablet computers</li> <li>b. Desktop and laptop computers</li> <li>c. Virtual desktops</li> <li>d. Servers on premise</li> <li>e. Co-located or hosted servers</li> <li>f. Cloud hosted servers</li> <li>h. Data in SaaS applications</li> </ul> </li> </ul>  | a.      |  |
| of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers Yes b. Desktop and laptop computers Yes c. Virtual desktops Yes d. Servers on premise Yes e. Co-located or hosted servers N/A f. Cloud hosted servers N/A g. Virtual machines Yes h. Data in SaaS applications N/A  |         | OWIT LOUIS!  |
| of the data to a server which is separated geographically from the system's normal operating location site.)  a. Mobile devices such as phones and tablet computers Yes b. Desktop and laptop computers Yes c. Virtual desktops Yes d. Servers on premise Yes e. Co-located or hosted servers N/A f. Cloud hosted servers N/A g. Virtual machines Yes h. Data in SaaS applications N/A  | 3 kand  | offsite data back-up a system in place for the following? (Offsite backup is the replication |
| location site.)  a. Mobile devices such as phones and tablet computers Yes b. Desktop and laptop computers Yes c. Virtual desktops Yes d. Servers on premise Yes e. Co-located or hosted servers N/A f. Cloud hosted servers N/A g. Virtual machines Yes h. Data in SaaS applications N/A   |         |  |
| <ul> <li>a. Mobile devices such as phones and tablet computers</li> <li>b. Desktop and laptop computers Yes</li> <li>c. Virtual desktops Yes</li> <li>d. Servers on premise Yes</li> <li>e. Co-located or hosted servers</li> <li>f. Cloud hosted servers N/A</li> <li>g. Virtual machines Yes</li> <li>h. Data in SaaS applications</li> </ul>   |         |  |
| b. Desktop and laptop computers Yes c. Virtual desktops Yes d. Servers on premise Yes e. Co-located or hosted servers N/A f. Cloud hosted servers N/A g. Virtual machines Yes h. Data in SaaS applications N/A  |         | ,  |
| c. Virtual desktops Yes d. Servers on premise Yes e. Co-located or hosted servers N/A f. Cloud hosted servers N/A g. Virtual machines Yes h. Data in SaaS applications N/A  |         |  |
| d. Servers on premise Yes e. Co-located or hosted servers N/A f. Cloud hosted servers N/A g. Virtual machines Yes h. Data in SaaS applications N/A  |         |  |
| e. Co-located or hosted servers NA f. Cloud hosted servers NA g. Virtual machines Yes h. Data in SaaS applications NA   | _       |  |
| f. Cloud hosted servers NA g. Virtual machines Yes h. Data in SaaS applications NA  |         |  |
| g. Virtual machines Yes h. Data in SaaS applications N/A  |         |  |
| h. Data in SaaS applications N/A  |         |  |
|   |         |  |
|   |         | ERP / finance system N/A   |

FOI Reference Number:

Issue Date:

Page 3 of 4

Any printed documents are considered uncontrolled. You must checkwith the current version on Staffnet.





- j. We do not use any offsite back-up systems
- 4. Are the services in question 3 backed up by a single system or are multiple systems used? Multiple systems are used
- 5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?
- 6. How many Software as a Services (SaaS) applications are in place within your organisation?
  - a. How many have been adopted since January 2020?

0

FOI Reference Number:

Issue Date:

Page 4 of 4

Any printed documents are considered uncontrolled. You must checkwith the current version on Staffnet.

