Freedom of Information requests concerning IT Security, Infrastructure, and Cyber Attacks

Tees Valley Combined Authority frequently receives Freedom of Information requests for information regarding our IT infrastructure systems, this can include security issues, including what systems we have in place, the suppliers, and versions. We are asked how often we update and amend our security, if we have identified any vulnerabilities and what we have done to strengthen any weaknesses. We believe providing this information could potentially allow individuals to identify issues and vulnerabilities with our IT systems.

The Authority has considered these issues carefully and we have decided we do not release information that would fall under this category of data. This is because we consider it is exempt under **Section 31 – Law Enforcement of the Freedom of Information Act 2000.**

IT Security Issues

We believe providing this information could potentially allow individuals to identify issues and vulnerabilities with our IT systems. Under the Freedom of Information (FOI) Act, the Authority is not just providing information to one individual, it is publishing the response to the world. There are individuals who will exploit system weakness to cause damage or defraud the organisation. If we provide information that informs criminals about our system updates for example, they can use this information to exploit any known weaknesses and hack systems.

Tees Valley Combined Authority uses all the necessary tools to keep our systems secure. A robust process is in place to ensure we regularly update and review guidance and consider current threats to the security of our data and systems to keep them safe.

We have a responsibility under the Data Protection Act 2018 to keep our customer and staff data secure, and we comply with that responsibility with appropriate technical and organisational measures that are in place.

While we value transparency in meeting our obligations, it is important that this is balanced against potential risk.

The Authority must take all necessary measures to keep our data and systems secure. This means not disclosing system information that would allow criminals to gain unlawful access to our systems.

Refusal notice: Section 31(1)(a) – Law Enforcement

The Authority does not release information that would identify issues or vulnerabilities of our IT systems, including details of suppliers and versions of our IT security, how often we update and amend our security and if we have identified fixes. We consider

disclosing this information would make the Authority a target of crime. Therefore, this information is exempt from disclosure under Section 31 of the Freedom of Information Act 2000.

Section 31(1)(a) says that we do not need to provide information that would be likely to prejudice the functions of law enforcement, the prevention and detection of crime. We believe that releasing this information places the Authority at risk and would increase the likelihood of criminals using the information to target attacks against Authority systems. The Authority must protect and safeguard the personal data it holds and not do anything which would allow personal data it to be accessed unlawfully. For example, knowing that last security update and version would allow criminals to know what vulnerabilities exist and target attacks on those.

Public interest test

As section 31 is a qualified exemption the public interest test has been applied:

Factors in favour of disclosure

- It would help transparency and accountability of the TVCA.
- It would reassure customers that our systems are secure
- It would provide information about how effective our security systems are

Factors in favour of non-disclosure

- There is an inherent public interest in crime prevention.
- There is a public interest in protecting the public money and avoiding costs associated with any attacks protecting the public purse.
- Public interest in protecting the non-financial cost to the Authority, such as reputational damage/publicity, distress, inconvenience and regulatory action associated with any attacks
- There is public interest in preventing threat to the integrity of Authority data
- There is public interest in ensuring the TVCA can comply with its duties to take all necessary steps to safeguard data.
- There is substantial public interest in ensuring that the Authority can continue to comply with its duties as a public Authority

On balance of the public interest test, we believe that public interest lies in upholding the exemption and not releasing the information.

Malware, ransomware attacks etc

We are frequently asked for information about malware, ransom ware, attacks and other cyber security incidents, including how many attacks, if they succeeded and the actions taken. The Authority has decided that we do not inform requesters if we hold this information or not. Under the Freedom of Information Act, this is a ‘neither confirm nor deny’ response. We apply this under section 31 of the act.

Refusal notice: Section 31(3)– Law Enforcement

The Authority does not release information that would allow cyber criminals insight into vulnerabilities which may or may not exist, this would likely damage our cyber security systems and plans. We consider disclosing any information would make the Authority a target for cyber-crime. Therefore, the Authority rely on section 31(3) of the Freedom of Information Act 2000. This allows the Authority to refuse to say if we hold any data and you should not assume that we do, or do not hold any data.

Public interest test

As section 31 is a qualified exemption the public interest test has been applied:

The public interest test is to determine if we should confirm if we hold the data or not, not whether we should disclose any data.

Factors in favour of disclosure

- It would help transparency and accountability of the TVCA.
- It would reassure customers that our systems are secure
- It would provide information about how effective our security systems are

Factors in favour of non-disclosure

- Confirming we hold information on how effective our security systems are would likely give cyber criminals insights into the strengths of Authority systems and highlight any potential weaknesses. This would increase the chances of a cyber-attack.
- The reasons that cyber security measures are in place is to protect the integrity of personal and official data, so increasing chances of a cyber-attack would have potential serious repercussions.
- There is a public interest in protecting the public money and avoiding costs associated with any attacks and protecting the public purse.
- There is public interest in protecting the non-financial cost to the Authority, such as reputational damage/publicity, distress, inconvenience and regulatory action associated with any attacks
- If the Authority were to confirm it held the data this could show criminals its systems are particularly vulnerable, encouraging attacks.
- There is a public interest in complying with our legal obligations to keep personal data secure and to take appropriate organisational and technical measures.

On balance of the public interest test, we believe that public interest lies in upholding the exemption and to neither confirm, nor deny we hold the data.

Cyber Attacks

We are asked for information relating to cyber-attacks experienced by the Authority.

The Authority does not hold a total number of attempted cyber-attacks. This is because the Authority is targeted daily with a wide range of cyber-attacks. Many are screened, isolated and/or repelled automatically by software and systems in place and are therefore not logged as individual 'incidents'.

Requests for the number and type of attack recorded by the Authority is withheld under section 31(3) of the Freedom of Information Act 2000. This allows the Authority to refuse to say if we hold any data and you should not assume that we do, or do not hold any data. At a time of heightened risk and cyber threat to UK government agencies, the Authority considers that disclosing this information would allow threat actors and groups to determine whether their attacks against ICT systems had gone undetected and from that point gauge the level of effectiveness of the Authority's cyber security measures.

Public interest test

As section 31 is a qualified exemption the public interest test has been applied:

The public interest test is to determine if we should confirm if we hold the data or not, not whether we should disclose any data.

Factors in favour of disclosure

- It would help transparency and accountability of the TVCA.
- It would reassure customers that our systems are secure
- It would provide information about how effective our security systems are

Factors in favour of non-disclosure

- Confirming we hold information on how effective our security systems are would likely give cyber criminals insights into the strengths of Authority systems and any potential weaknesses. This would increase the chances of a cyber-attack.
- The reasons that cyber security measures are in place is to protect the integrity of personal and official data, so increasing chances of a cyber-attack would have potential serious repercussions.
- There is a public interest in protecting the public money and avoiding costs associated with any attacks and protecting the public purse.
- If the Authority were to confirm it held the data this could show criminals its systems are particularly vulnerable, encouraging attacks.
- There is a public interest in complying with our legal obligations to keep personal data secure and to take appropriate organisational and technical measures.

On balance of the public interest test, we believe that public interest lies in upholding the exemption and to neither confirm, nor deny we hold the data.

Right of Internal Review

If you are unhappy with the way your request for information has been handled, you may request an Internal Review within 40 working days by writing to:

TVCA Chief Executive, Tees Valley Combined Authority, Teesside Airport Business Suite, Teesside International Airport, Darlington. DL2 1NJ. Please quote your FOI reference number.

If, after your complaint has been determined, you remain dissatisfied with the handling of your request or complaint, you have a right to appeal to the Information Commissioner at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113