



Llywodraeth Cymru
Welsh Government

Our ref: ATISN 11484

Date: 13 September 2017

Dear,

Request for Information – ATISN reference 11484

Thank you for your request which was received by the Welsh Government on 16 August 2017.
You asked for the following information:

- How regularly did we undertake audits of the keys and certificates between 1st August 2016 and 31st July 2017;
- How often do we you change or rotate keys and certificates;
- The number of times we have detected people attempting to use unauthorised devices on our system between 1st August 2016 and 31st July 2017;
- The date of the last update to our documented framework covering policies related to information security relating to the PKI; and
- How often do you undertake an audit of certificates & PKI data and the date this was last undertaken.

I have decided that I can neither confirm or deny, under s31(3) and s24(2) of the Freedom of Information Act 2000 (FOIA), we hold any information that matches the description of the information you have sought. A description of my application of these exemptions are set out in Annex A to this letter.

If you are dissatisfied with the Welsh Government's handling of your request, you can ask for an internal review within 40 working days of the date of this response. Requests for an internal review should be addressed to the Welsh Government's Freedom of Information Officer at:

Information Rights Unit,
Welsh Government,
Cathays Park,
Cardiff,
CF10 3NQ

or

Email: FreedomOfInformationOfficer@wales.gsi.gov.uk

Please remember to quote the ATISN reference number above.

You also have the right to complain to the Information Commissioner. The Information Commissioner can be contacted at:

Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.

However, please note that the Commissioner will not normally investigate a complaint until it has been through our own internal review process.

Yours sincerely

Annex A

Section 24(2) of the FOIA provides an exemption to the duty to confirm or deny whether the requested information is held where doing so would compromise national security.

The application of this exemption requires that we consider whether the wider public interest in being exempt from that duty to confirm or deny we hold any such information outweighs any public interest arguments in favour of complying with that duty.

We recognise that the one of the primary concerns of government, at all levels, is to ensure the safety of its constituents and the country. There is a public interest in knowing that government works to ensure the country and its citizens are kept safe and secure and the security of cyberspace is a key component of that ongoing vigilance.

However, where the disclosure of any information, no matter how trivial that information may seem, has the potential to undermine and put at risk the security of the state, the wider public interest weighs heavily in favour of the non disclosure of that information.

Section 31(3) of the FOIA provides an exemption to the duty to confirm or deny whether the requested information is held where doing so would, or would be likely to, prejudice the prevention or detection of crime (s31(1)(a) FOIA).

The application of this exemption requires that we consider whether the wider public interest in being exempt from that duty to confirm or deny we hold any such information outweighs any public interest arguments in favour of complying with that duty.

As indicated above, the public interest in non disclosure of any information which potentially could compromise the security of government cyberspace and thereby increasing the risks to its citizens that they could become the victim of crime, or could negatively impact the ability of the law enforcement agencies to detect and apprehend criminals, clearly outweighs any public interest in disclosure.