



## Senedd Core Systems

24 August 2023

### Request for Information.

Thank you for your request received on 3 August 2023 in which you asked:

*Hi, Could you please respond to the following questions about your Core Systems:*

**1.** *How many employees do you have?*

**2. ERP**

- Which Enterprise Resource Planning (ERP) or Finance system do you currently use?*
- What is the value & expiry date of your current contract/licence? What are the extension options?*
- Do you have any plans to review (upgrade/change) this system?*

**3. CRM**

- Which Customer Relationship Management (CRM) System do you currently use?*
- What is the value & expiry of your current contract/licence? What are the extension options?*
- Do you have any plans to review (upgrade/change) this system?*

**4. SCM**

- Which Supply Chain Management (SCM) System do you currently use?*
- What is the value & expiry date of your current contract/licence? What are the extension options?*
- Do you have any plans to review (upgrade/change) this system?*

**5. EPM**

- Which Enterprise Performance Management (EPM), Scenario Planning or Strategic Modelling System do you currently use?*
- What is the value & expiry date of your current contract/licence? What are the extension options?*

Senedd Cymru  
Bae Caerdydd  
Caerdydd, CF99 1SN

Welsh Parliament  
Cardiff Bay  
Cardiff, CF99 1SN  
Ffôn/Tel: 0300 200 6544

E-bost/Email: [Ceisiadau-gwybodaeth@senedd.cymru](mailto:Ceisiadau-gwybodaeth@senedd.cymru)  
[Information-request@senedd.wales](mailto:Information-request@senedd.wales)

- *Do you have any plans to review (upgrade/change) this system?*

## **6. HR & Payroll**

- *Which Human Capital Management (HCM) or HR and Payroll system do you currently use?*
- *What is the value & expiry date of your current contract/licence? What are the extension options?*
- *Do you have any plans to review (upgrade/change) this system?*

## **7. BI**

- *Which Analytics or Business Intelligence Systems do you currently use?*
- *What is the value & expiry date of your current contract/licence? What are the extension options?*
- *Do you have any plans to review (upgrade/change) this system?*
- *Do you have any plans to migrate to a fully integrated, fully cloud-based back-office system in the next two years?*

We confirm we hold some of the information requested. However, a full disclosure will not be made on this occasion because some of the information requested is exempt from disclosure under the Freedom of Information Act 2000 ("the Act").

Please find attached an Excel spreadsheet that contains our responses to your request. The spreadsheet sets out the information that:

- we are able to disclose;
- we do not hold (denoted by 'N/A');
- is published on our website via our **contract schedule** (and which is thereby exempt from disclosure by virtue of section 21 of the Act which covers information accessible by other means); and
- is exempt from disclosure by virtue of alternative exemptions (denoted by 'withheld').

We consider that providing you with a full disclosure would indicate how we manage our internal secure systems which would, in turn, make those systems vulnerable to malicious attacks. To this end, we consider two exemptions apply which, in brief, are as follows:

1. section 24 – withholding the information is required for the purpose of safeguarding national security; and
2. section 31(1)(a) – disclosure of the information would, or would be likely, to prejudice the prevention of crime.

Fuller details of the exemptions which have been applied, and the reasons for their application, are set out in the annex to this letter.

Yours sincerely

**Buddug Saer**  
**Freedom of Information Manager**  
**Welsh Parliament**

Your request has been considered according to the principles set out in the **Code of Practice on Public Access to Information**. If you have any questions regarding this response please contact me. If you feel you have cause for complaint, please follow the guidance below.

Cause for concern or complaint with your FOI response?

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

**Information-request@senedd.wales** or in writing to

Welsh Parliament  
Governance and Assurance  
Cardiff Bay  
Cardiff  
CF99 1SN

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at:

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

## Annex

### Section 31

Section 31(1) of the Act provides:-

- *Information which is not exempt information by virtue of section 30 is exempt information if the disclosure would, or would be likely to, prejudice –  
(a) the prevention or detection of crime...*

The operation of this exemption involves a number of steps:

- one of the law enforcement interests protected by section 31 must be harmed (or “prejudiced”) by the potential disclosure;
- the prejudice claimed must be real, actual or of substance;
- the public authority must be able to demonstrate a causal link between the disclosure and the prejudice claimed;
- the public authority must then decide what the likelihood of the prejudice occurring would be in the event of a disclosure being made (i.e. would it occur, or would it only be likely to occur).

The more likely the prejudice, the greater the weight it carries when considering the public interest. In this context, the term “would prejudice” means that it has to be more probable than not that the prejudice would occur. “Would be likely to prejudice” is a lower level.

Information can only be withheld under section 31 if its disclosure would, or would be likely to, prejudice one of the activities listed in either subsection (1) or (2). The relevant activity here is “the prevention or detection of crime” as listed in subsection (1)(a).

Section 31(1)(a) covers all aspects of the prevention and detection of crime. This exemption may be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime. So, the public authority may rely on the exemption in order to protect information on or about its systems, where the disclosure of that information would make it (and others) more vulnerable to crime. The information covered by this exemption is the identity of the providers of software and operating

systems in use by the Senedd Commission ("Commission"), which in turn would disclose key information about those systems, the versions in use, including the operating systems and infrastructure services.

The factors against disclosure include:

- the Commission has a duty as a controller under data protection law to ensure the security of all of the personal data that we hold. Making a disclosure would undermine our ability to meet that duty by, for example, rendering the systems more vulnerable to attack; and
- a disclosure would leave our data vulnerable to access, disclosure, alteration or destruction. In turn this may lead to crimes including offences against property, offences against persons, public order offences, fraud, or digital vandalism.

The prejudice test is not limited to the harm caused by the requested information on its own. Account can be taken of any harm likely to arise if the requested information were put together with other information already known to the requester or in the public domain. It is also appropriate to consider the precedent that could be set for future requests by disclosing information about our security arrangements.

Our view, having considered the effect that disclosure would have on the integrity of the Commission and its ICT infrastructure, is that to disclose the withheld information would place at risk the security of the Commission's systems and, as a result of that, the security of the Commission, the Senedd, those who work on and visit the Senedd estate, as well as those who work with us. This would prejudice the prevention or detection of crime.

We then went on to consider the public interest test. As part of this test, there is a need to balance the security of the Senedd and the Commission, and its ICT infrastructure, as against the public interest in holding the Commission to account.

There is a clear public interest in the Commission being transparent in its processes and systems so that it can be held to account as a public authority. However, there is also a clear public interest in protecting society from the impact of crime. Additionally, there is a public interest in enabling the Commission to fulfil its functions and purpose. The Commission has a duty to provide to the Senedd the services it requires to perform its functions. A disclosure would undermine our ability to meet that duty because, for

example, the core systems in operation would cease to function effectively and appropriately if subject to attack.

The greater the potential for a disclosure to result in crime, the greater the public interest in maintaining the exemption. The victims of crime can be both organisations and individuals, but, in our view, there is a greater public interest in protecting individuals from the impact of crime. By disclosing information that could allow the identification of vulnerabilities in the Commission ICT infrastructure, the individuals who work on and visit the Senedd estate would be placed at a greater risk of crime. In addition, individuals and organisations who engage with our outreach team, communications team and committee service could also be put at risk, if our systems were ever compromised. This would also be the case for any external contractors and suppliers with whom we engage.

In this case, it is our view that the public interest in favour of disclosure does not outweigh the need to protect the integrity of the ICT infrastructure in place to protect the Commission and Senedd, those who work for us, and those who work with us.

## Section 24

Section 24(1) of the Act provides:-

- *Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security.*

We consider it necessary to withhold the information in order to maintain the integrity and robustness of the ICT infrastructure of the Commission and all of the data, including personal data, that is held within it. In turn, this enables us to ensure the safe and effective functioning of the Senedd as a legislature.

The information covered by this exemption relates directly to specific software and operating systems in use by the Commission. It includes systems used by the Commission's HR and Finance teams, each of which is critical to the effective and efficient functioning of the Commission. Disclosing details of the specific systems in use would make it easier for an attacker to exploit those systems as well as other systems on the network which hold a variety of information including medical, financial and other personal information.

Were those systems to be compromised by a traversal attack, where accessing one application can then leave others under threat, our resources and data would be vulnerable to access, disclosure, alteration or destruction. The risk in the disclosure of this information is that there is a genuine likelihood it would damage the effectiveness and integrity of those systems and, in turn, impair the functioning of the Commission and the Senedd.

The integrity and robustness of our ICT systems is paramount to the functioning of both the Commission and the Senedd. Although your request has not asked for information relating specifically to the CCTV systems in operation, it has been identified as an example of a system that could be accessed, if other systems such as Finance and HR were compromised. We are categorised as a **Tier 1 Site** and the operation of the CCTV system is an example of the need to maintain the integrity of our ICT system in order to ensure the security of the estate. Were the CCTV and access control systems to be



impaired, there is a real possibility that it would leave the Senedd estate extremely vulnerable, as we would not be able to identify any hostile approaches or manage any unlawful activities. By maintaining effective controls we are able to ensure that Senedd Members, Senedd Member Support Staff, Senedd Commission staff, and visitors to the Senedd estate are not put at risk.

This exemption is a qualified exemption, and as such, the public interest in upholding the exemption must be considered. The key public interest consideration for disclosure is that the public have a right to know that there are adequate and appropriate ICT systems in place in the Commission and the Senedd. It is our opinion, however, that the release of the withheld information would materially damage the integrity and effectiveness of the Senedd's ICT security arrangements and systems and therefore, in this instance, the public interest in withholding the requested information outweighs the public interest in its disclosure.