Electronic Signature Security Tips

With the transition to work from home there is an increased need of agencies abilities to obtain signatures of documents. This bulletin serves as a guide in what to look for when considering electronic signature applications.

The State does not currently support specific electronic signature tools. Feel free to share these tips with whomever you wish.

Cyber Security Services (CSS) recommends exercising due diligence and caution in your cybersecurity efforts. Therefore, it is important to consider the classification level of the data in question (Data Classification Policy 107-004-050: http://www.oregon.gov/das/Policies/107-004-050.pdf).

Choosing a solution is a business decision, however EIS/CSS is here to assist, review and provide guidance pertaining to potential security risks before procurement. The following steps can be taken when determining which solution/tool or application fits your agency's needs.

Electronic signature Best Practices:

For Level 1 & 2 data:

- If the solution/tool or application is low risk, low cost and the need is due to COVID-19 remote work, CSS will review and return request within 24 business hours.
- Completion of a cloud workbook is suggested and you may send it to ESO.Info@oregon.gov if you wish to have assistance or security guidance provided.
- Attach vendor Terms of Use or any other vendor type of contract being enter into.
- Depending if regulated data applies, DOJ may need to review vendor contract and provide a legal sufficiency opinion.
- We still encourage a review of where the data is stored for level-2 data. Overseas storage is discouraged in many cases.

For Level 3 & 4 data:

- Completion of a cloud workbook is required, please reach out to the ESO.Info@oregon.gov for security assistance.
- Attach vendor Terms of Use and any other vendor contract.
- If regulated data applies, DOJ will need to review.

- When looking at purchasing options, determine if a government version is available, which may better suit agency's needs.
- Solutions that will process and/or store level-3 or higher data will still need to meet legal sufficiency review with the DOJ, such that they will need to agree to the terms that are set out in the IT Rider or Contract templates.
- Some key considerations are compliance with our statewide standards, domestic data storage and access, auditing, and breach notifications (to name a few).

In all cases:

- Administrative user management: Usernames and password are now covered under Oregon's Privacy law (OCITPA: ORS 606A.600), so, proper protection and management of these credentials needs to be highlighted. Each vendor must comply with OCITPA.

Below are a few tools/applications the EIS/CSS BISO team has reviewed:

DocuSign:

- ISO20071:2013 certified
- SOC 1 Type 2, SOC 2 Type 2 certified organization. They report they have year audits across all aspects of their production operations, including their datacenters, and have sustained and surpassed all requirements.
- PCI-DSS compliant
- They adhere to CSA-STAR requirements.
- https://www.docusign.com/sites/default/files/Trust-Brief-TB051319TCAPUBGLB.pdf
- https://www.docusign.com/sites/default/files/DS_SecurityBrief_SB_051519_IS_PUB_GLB.pdf
- https://www.docusign.com/company/terms-and-conditions/web
- https://www.docusign.com/products-and-pricing

Adobe Sign:

- Adobe Sign is certified compliant with the world's most rigorous security standards, ISO 27001, SOC 2 Type 2, and PCI DSS used in the payment card industry. It complies with a wide range of privacy regulations, including HIPAA, GLBA, and FERPA in the U.S.
- https://www.adobe.com/legal/terms.html
- https://www.microsoft.com/en-us/industry/microsoft-adobe-enterprise-partnership?activetab=pillars:primaryr2

Written 05/12/2020