Duke Services and Data Classification [1]

Version 1.2

Author

Duke University IT Security Office (ITSO)
Duke Health Information Security Office (ISO)

Authority

Duke University Chief Information Security Officer
Duke Health Chief Information Security Officer

Determining the Nature of the Data

Questions to Consider


Use of Duke Services

Selecting a Duke Service Depending on Data Classification

The following chart outlines which Duke services meet the minimum security requirements for use with Sensitive, Restricted and Public data. (Staff can also use the SecureIT [8] decision tree tool.) Duke faculty, students and staff should be aware that there may be institutional, legal, regulatory and contractual obligations [9] that require the use of specific storage options. For
example:

- ITAR and PCI-related data always require Security Office consultation before use.
- FERPA: Consult with the Registrar’s Office [6].
- FISMA and Veterans Administration: PACE is required storage. REDCap is not allowed.
- Social Security Numbers: Collection requires an institutional exception [3].
- GDPR: Consult with the Privacy Office for allowable options [10].
- Duke Health non-consented clinical research data: PACE is required storage.

All users of the solutions and services that store Duke data must adhere to the following:

- Use only for the approved intended use.
- Store only the information you need or plan to use.
- Provide access only to authorized or approved individuals; remove access immediately when no longer need.
- Do not provide public or broad access to data without institutional approval
- Retain data only as long as it is needed, or in accordance with Duke retention requirements.
<table>
<thead>
<tr>
<th>Service</th>
<th>Available to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duke OIT CIFS/NFS Home Drive Service</td>
<td>Duke University</td>
</tr>
<tr>
<td>Duke OIT &amp; Departmental File Shares</td>
<td>r,p</td>
</tr>
<tr>
<td>Duke University Protected Network</td>
<td>Duke University</td>
</tr>
<tr>
<td>Duke University Protected Research Data Network</td>
<td>s,r</td>
</tr>
<tr>
<td>Duke Compute Cluster</td>
<td>Duke University</td>
</tr>
<tr>
<td></td>
<td>s,r</td>
</tr>
<tr>
<td>DHTS Home Drive Service</td>
<td>Duke Health</td>
</tr>
<tr>
<td></td>
<td>s,r</td>
</tr>
<tr>
<td>Duke Health Network Storage</td>
<td>Duke Health</td>
</tr>
<tr>
<td></td>
<td>r,p</td>
</tr>
<tr>
<td>Duke Health CITRIX VDI</td>
<td>Duke Health</td>
</tr>
<tr>
<td></td>
<td>s,r</td>
</tr>
<tr>
<td>Duke Health Protected Analytics Compute Environment (PACE)</td>
<td>Duke Health</td>
</tr>
<tr>
<td></td>
<td>s,r</td>
</tr>
</tbody>
</table>
Use of Cloud Services

Selecting a Cloud Service Depending on Data Classification

The following chart outlines which Duke services are appropriate for use with Sensitive, Restricted and Public data.

<table>
<thead>
<tr>
<th>Service</th>
<th>Available to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duke's Box Service*</td>
<td>Duke University Duke Health</td>
</tr>
<tr>
<td>Duke's Qualtrics Service</td>
<td>Duke University Duke Health</td>
</tr>
<tr>
<td>Duke's Microsoft OneDrive Service*</td>
<td>Duke University Duke Health</td>
</tr>
<tr>
<td>Service</td>
<td>Owner</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Duke's Jabber</td>
<td>Duke University Duke Health</td>
</tr>
<tr>
<td>Duke's Zoom ***</td>
<td>Duke University Duke Health</td>
</tr>
<tr>
<td>Duke's Zoom Telehealth***</td>
<td>Duke Health</td>
</tr>
<tr>
<td>Duke's WebEx ***</td>
<td>Duke University Duke Health</td>
</tr>
<tr>
<td>Duke University Adobe Sign ****</td>
<td>Duke University Duke Health</td>
</tr>
<tr>
<td>Duke Health Adobe Sign ****</td>
<td>Duke Health</td>
</tr>
<tr>
<td>Cloud tenants (including Amazon Web Services, Azure, Google Cloud Platform)</td>
<td>Duke University Duke Health</td>
</tr>
</tbody>
</table>

*No ITAR or PCI related data may be stored on Box or Microsoft Office 365. For additional details see: [https://box.duke.edu/security-and-usage/](https://box.duke.edu/security-and-usage/) [11]

**If the Team will be used to share Sensitive Data, the Team must be set to Private not Public.*** Duke Health may use Zoom for classes and meetings but NOT for clinical purposes to see patients or exchange Protected Health Information (PHI). Any meeting with the possibility of PHI may not be recorded. Sensitive information may be discussed during a live Zoom meeting when recording is not in use but should not be recorded, typed into a chat session or otherwise stored within Zoom. [12]

***Specific guidelines exist for the use of Adobe Sign. For more see General Information and License Restrictions [13]. Note: All Health side access for Adobe Sign must be approved and provisioned by DHTS Web Services.

Use of Other Cloud Services (Personal Use)
Selecting a Cloud Service Depending on Data Classification

The following chart outlines outside cloud services appropriate for personal use. In general, these services are not approved for official Duke use without consultation with the Duke security offices and/or privacy offices.

<table>
<thead>
<tr>
<th>Service</th>
<th>Available to:</th>
<th>DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iCloud</td>
<td>Personal</td>
<td>p</td>
</tr>
<tr>
<td>Personal Box Account</td>
<td>Personal</td>
<td>p</td>
</tr>
<tr>
<td>Personal OneDrive Account</td>
<td>Personal</td>
<td>p</td>
</tr>
<tr>
<td>DropBox</td>
<td>Personal</td>
<td>p</td>
</tr>
<tr>
<td>Google Apps (including Gmail)</td>
<td>Personal</td>
<td>p</td>
</tr>
<tr>
<td>Facebook (including Workplace)</td>
<td>Personal</td>
<td>p</td>
</tr>
<tr>
<td>Slack</td>
<td>Personal</td>
<td>p</td>
</tr>
</tbody>
</table>

Document Type: Policy
Applicable To: Duke Health
Source URL: https://security.duke.edu/policies/duke-services-and-data-classification

Duke University
Links
[4] https://security.duke.edu/copyrightdmca
[8] https://secureit.duke.edu/data_services
[10] https://oarc.duke.edu/privacy