DoWEA Cloud Questionnaire

Directions

The Department of Defense Education Activity (DoWEA) must review each vendor's cloud-based solution individually to determine if it is compatible with DoD and DISA's guidelines. Your answers to this questionnaire will enable us to do that evaluaton quickly and effectively. Please provide the point(s) of contact should DoWEA have questions about your response.

Please note:

- Any proprietary or sensitive security information provided in response to this questionnaire will be protected and not shared outside of the US Government.
- Links to web-pages will be considered an unacceptable answer to the question but can be provided as supporting documentation.
- Not answering a question will be considered an unacceptable response.

Cloud Resource Website/URL's

1. Are Cloud Resources URLs provided for this solicitation? (Yes or No) **Select Item**
2. Has access to the Cloud Resource been supplied for this solicitation for review? (Yes or No) **Select Item**
3. Please provide all URLs for this resource.

Client Systems and Software Configuration (3 Questions)

1. Will DoWEA need to stand up servers to support this application? (Yes or No) **Select Item**
2. Is any software required for this service, e.g., software that must be installed on DoWEA computers to include browser extensions and/or plugins? (Yes or No) **Select Item**
    a. If Yes, has this software been made available for this review? (Yes or No) **Select Item**
3. Are there any configurations or changes that DoWEA must implement to any of its computers, browsers or firewalls to utilize this service? (Yes or No) **Select Item**

Privacy Information Data Collection and Distribution (6 Questions)

1. Is Personally Identifiable Information (PII) and/or sensitive information collected by this service? (Yes or No) (Some examples of PII: Full name, Home address, Work Address, Email address, Social security number, Passport number, Driver's license number, Date of birth, Gender, Telephone number) **Select Item**

2. Is any, personally identifiable and sensitive information collected by third parties or by external business partners (e.g., via cookies, plug-ins, ad networks, web beacons etc.)? (Yes or No) **Select Item**

3. Is any DoWEA data provided to third parties or external business partners for any purpose? (Yes or No) **Select Item**
   a. If yes provide a list of all third-party or external business partner recipients.

4. Do third parties or external business partner recipients of DoWEA data adhere to the same policies and processes to protect DoWEA data? (Yes or No) **Select Item**

5. Is there a **process** to opt-out of any transfers of DoWEA data to third parties or external business partner recipients? (Yes or No) **Select Item**

6. Are the following requirements for your cloud service meet?
   a. Children's Online Privacy Protection Act (COPPA), per https://www.congress.gov/bill/105th-congress/senate-bill/2326/text (Yes or No) **Select Item**
   b. Privacy Act of 1974, per https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition (Yes or No) **Select Item**
   c. Family Educational Rights and Privacy Act (FERPA), per https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (Yes or No) **Select Item**
   d. Children's Internet Protection Act (CIPA), per http://www.fcc.gov/guides/childrens-internet-protection-act? (Yes or No) **Select Item**

System Management and Security (7 Questions)

1. Do you perform **system** penetration testing? (Yes or No) **Select Item**

2. Do you perform **application** penetration testing? (Yes or No) **Select Item**

3. Is application penetration testing performed after code changes? (Yes or No) **Select Item**

4. Do you perform regular system vulnerability testing? (Yes or No) **Select Item**

5. Do you have system intrusion prevention in place? (Yes or No) **Select Item**

6. Are system software updates and patches provided? (Yes or No) **Select Item**

7. Is the system, including its server(s) and network devices, located in an environmentally controlled and secure facility under controlled circumstances (e.g., authorized personnel access lists, ID cards, entry logs)? (Yes or No) **Select Item**

Data Storage, Retention, and Access (10 Questions)

1. Is DoWEA's information and data stored in the United States, to include outlying areas or DoD on-premises? (Yes or No) **Select Item**

2. Are all the Offeror's employees and/or subcontractors that have or will be accessing DoWEA's data located within the United States? (Yes or No) **Select Item**

3. Will any Sensitive and/or Confidential data including but not limited to PII data be transferred? (Yes or No) **Select Item**

4. Will DoWEA's data at rest be encrypted? (Yes or No) **Select Item**

5. Is the system/database hosted on a multi-tenant instance? (Yes or No) **Select Item**

6. Is data secured with unique encryption keys for each customer on systems hosting multiple customers? (Yes or No) **Select Item**

7. Will DoWEA's data be protected in transit, e.g., secure socket layer (SSL), hashing, etc.? (Yes or No) **Select Item**

8. Are background checks completed on personnel to include subcontractors with access to servers, applications, and customer data? (Yes or No) **Select Item**

9. Is there a **process** for authenticating callers and resetting access controls? (Yes or No) **Select Item**

10. Is there a process to delete school/system data? (Yes or No) **Select Item**

Development and Change Management Process (4 Questions)

1. Is there a customer notification process for any changes made to corporate policies for data protection? (Yes or No) **Select Item**

Audits and Standards

2. Is there a process for DoWEA to audit the security and privacy of records? (Yes or No) **Select Item**

3. Are the security operations reviewed or audited by an outside group? (Yes or No) **Select Item**

4. Are any security standards followed? (Yes or No) (Example: International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST) and Payment Card Industry Data Security Standards (PCI DSS)) **Select Item**

Test and Development Environments (1 Question)

1. Will "live" student/privacy data be used in a non-production environment, e.g., in testing, development, or training)? (Yes or No) **Select Item**

Data Breach, Incident Investigation and Response (4 Questions)

1. Is there a backup-and-restore process in case of a disaster? (Yes or No) **Select Item**
2. Is there protection in place against denial-of-service attack? (Yes or No) **Select Item**
3. Is there **process** in managing a **data** breach? (Yes or No) **Select Item**
4. Is there a **process** in performing security incident investigations and/or e-discovery (different from a data breach)? (Yes or No) **Select Item**

Please provide any Additional if needed.