ellucian

Information Security Agreement

This Schedule D to Exhibit 1 contains terms governing information security to which Ellucian will adhere during the Hosting Services Term. Ellucian may modify specific security protections from time to time, but will continue to provide at least the same level of security as on the date this Schedule D became part of the Agreement.

1. Information Security Program

Ellucian will maintain a global Information Security Program aligned with ISO 27001 that will plan, implement and manage processes on an ongoing basis to meet information security objectives and requirements applicable to the Hosting Services delivered worldwide. The Information Security Program will include demonstrable oversight and commitment from Ellucian senior management. The Information Security Program will also include performing information security risk assessments and implementing treatment plans at appropriate intervals, such as when significant changes to the Hosting Services occur.

2. Information Security Compliance

Ellucian will design and maintain a control environment for the Hosting Services aligned with global information security practices and standards such as ISO 27001 and third party attestation frameworks such as SSAE 16 / SOC 1 and SOC 2.

3. Information Security Policy

Ellucian will maintain an Information Security Policy that is approved by senior management and communicated to employees and applicable third parties. The Information Security Policy will identify roles and responsibilities as well as governing principles and control objectives for information security across Ellucian's global business operations. The Information Security Policy and will be reviewed annually and supporting standards, guidelines and procedures will be adjusted as appropriate.

4. Information Security Awareness Program

Ellucian will maintain an employee awareness program to allow employees to understand and fulfill their responsibilities for information security, including requirements for personal data privacy, confidentiality, and non-disclosure of information.

5. Personnel Security

Employees will be screened in accordance with relevant laws and such screening will be proportional to employee roles and responsibilities. Employees and applicable third parties will agree to requirements for confidentiality and non-disclosure of information prior to employment or prior to providing services to Ellucian.

6. Physical Security

Ellucian currently uses Amazon Web Services (AWS) who is responsible for protecting the global infrastructure upon which the Hosting Services are delivered. AWS will maintain controls to manage and monitor physical access at both the data center perimeter and building ingress points using security staff, or electronic access control validation.

7. Access Control

Ellucian will authorize access to the Cloud Environment only for employees and third parties with a legitimate business need. Controls and mechanisms to authenticate access and monitor and prevent unauthorized access to

Client's Systems will also be in place. Ellucian will also maintain appropriate onboarding and termination processes to manage revocation of access to Client's Systems.

8. Data Security

Ellucian will maintain security controls to safeguard Client's Systems from unauthorized access, modification, disclosure or destruction, or become inaccessible to authorized users. Data protection methods will include restricting and monitoring access to information systems, encrypting data in transit and while at rest when necessary or required, maintaining backups of Client's Systems, and securely returning data to the Client, or disposing or destroying data in a secure manner using techniques consistent with NIST 800-88 ("Guidelines for Media Sanitization").

9. Client's System Security

Ellucian will protect the confidentiality, integrity and availability of Client's Systems. Ellucian will maintain safeguards for the security of electronic communications networks. Ellucian will also maintain a change management process to control planned and unplanned changes and the installation of software, manage mechanisms to detect threats such as malware, and recording and monitoring security events to identify anomalous or unauthorized activity.

10. Technical Vulnerability Management

Ellucian will maintain a process and supporting tools to evaluate and resolve technical vulnerabilities within Client's Systems within reasonable timeframes to address the risk of potential exploitation, or system or data compromise.

11. Third Party Security

Ellucian will maintain a process to identify risks to Client's Systems that are accessible to third parties. The process will ensure that relevant information security requirements are incorporated into business agreements with third parties and that relevant third party risks are addressed within reasonable timeframes.

12. Information Security Incident Management

Ellucian will maintain an information security incident management program to respond to security incidents within the Cloud Environment. Ellucian will provide timely notification to the Client in the event that Client's Systems or data is known to have suffered an Information Security Breach. Timely notification is defined as providing notice to the Client as soon as reasonably practicable and without undue delay after Ellucian became aware of the Information Security Breach. An "Information Security Breach" is defined as an event(s) that is known to have resulted in unauthorized access to a Client's System, or use or disclosure of Client data. Ellucian will further maintain a process to capture and apply knowledge gained from such events to address the likelihood of reoccurrence.

13. Business Continuity Management

Ellucian will implement controls designed to maintain the continued availability of Client's Systems. Controls will include maintaining a defined business continuity management plan relevant to the Hosting Services that, if interrupted, may result in significant downtime or data loss.