U.S. Department of Education's
Federal Student Aid (FSA) Partner Connect System and User Access Management

Authorizing Official Designation

Organization Name:

Organization Code:

Certification of the President/Chief Executive Officer (CEO) or Designee

Responsibilities of the President/CEO or Designee

As the President/CEO or Designee, I certify that:

- Consistent with the U.S. Department of Education's Terms of Service for our systems, my organization will not permit unauthorized use or sharing of log in credentials that have been issued to anyone at my organization and will take immediate action to remedy any such unauthorized use or sharing that is identified.
- Each individual who is an Administrator, SAIG Mailbox User, and/or Partner User for my organization has read and acknowledged the "*Responsibilities of FSA Partner Connect Users*."
- My organization has provided for the security, confidentiality, and integrity of student information, protected against any anticipated threats or hazards to the security or integrity of such information; and protected against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any student (16 C.F.R. §314.3(b)). My organization further verifies that administrative, operational, and technical security controls are in place and are operating as intended pursuant to the Federal Trade Commission's (FTC) Final Rule on Standards for Safeguarding Customer Information (i.e., the Safeguards Rule). Additionally, my organization verifies that it has performed appropriate due diligence to ensure that, at a minimum, any employee who has access to Federal Student Aid (FSA) Institutional Student Information Record (ISIR) data, including federal tax information (FTI), meets applicable federal and state security requirements for personnel handling controlled unclassified information (CUI) and sensitive personally identifiable information (SPII), including but not limited to meeting the requirements under 26 U.S.C. §6103(l)(13), 20 U.S.C. §1098h, and IRS Publication 1075 if applicable.
- My organization has ensured the standards for protecting federal tax information (FTI) have been implemented according to Internal Revenue Code (IRC) 26 U.S.C. §6103 – Confidentiality and disclosure of returns and return information and pursuant to 20 U.S.C.§1090, Section 483 of the Higher Education Act, as amended – Use of FTI and *Free Application for Federal Student Aid* (FAFSA®) data. I further acknowledge violations of the IRC may lead to criminal and/or civil penalties pursuant to 26 U.S.C. §§7213, 7213A, and 7431. Penalties apply to willful unauthorized disclosure and inspection of tax return or return information with punishable fines or imprisonment. Additionally, I further acknowledge a taxpayer may bring civil action for damages against an officer or employee who has inspected or disclosed, knowingly or by reason of negligence, such taxpayer's tax return or return information in violation of any provision of IRC §6103.
- I understand the Secretary may consider any unauthorized disclosure or breach of student records and student applicant information as a demonstration of a potential lack of administrative capability on the part of an institution of higher education under 34 C.F.R. §668.16. I further understand that in the event of an unauthorized disclosure or breach of student applicant information or other sensitive information (such as personally identifiable information), the Administrator or the Qualified Individual identified under 16 C.F.R. Part 314 must notify Federal Student Aid by submitting the Cybersecurity Breach Intake Form on FSA Partner Connect as soon as possible, but no later than 24 hours after the incident is known or identified. I am responsible for ensuring that any unauthorized disclosure or breach of student applicant information or other sensitive information (such as personally identifiable information) is reported to Federal Student Aid as required. I understand that my organization must cooperate with the Department and provide any requested information regarding an unauthorized disclosure or breach as well as report any breach that occurs at my organization's third-party providers that maintain, store, or otherwise utilize the data. I understand that any information that is provided to third parties by my organization is also covered by these same provisions.
- I have ensured that the Standards for Safeguarding Customer Information (as the term customer information applies to my organization), 16 C.F.R. Part 314, issued by the Federal Trade Commission (FTC), as required by the Gramm – Leach – Bliley Act (GLBA), P.L. 106-102 have been implemented and understand that these Standards provide, among other things, that I implement the following and I understand that failure to implement the requirements of the GLBA may be considered a lack of administrative capability under 34 C.F.R. §668.16 by the Secretary. I further acknowledge that my responsibility to safeguard customer information extends beyond Title IV, Higher Education Act program recipients:
  - Develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts that meets the requirements for an information security program in 16 C.F.R. Part 314.
  - Designate a qualified individual responsible for overseeing an implementing my organization's information security program and enforcing my organization's information security program in compliance with 16 C.F.R. §314.4(a).
  - Base my organization's information security program on a risk assessment that identifies reasonably foreseeable internal

and external risks to the security, confidentiality, and integrity of customer information (as the term customer information applies to my organization) that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks as required under 16 C.F.R. §314.4(b).

- Design and implement safeguards to control the risks my organization identifies through risk assessment that meet the requirements of 16 C.F.R. §314.4(c)(1) through (8).
- Regularly test or otherwise monitor the effectiveness of the safeguards my organization has implemented that meet the requirements of 16 C.F.R. §314.4(d).
- Implement policies and procedures to ensure that personnel are able to enact my organization's information security program and meet the requirements of 16 C.F.R. §314.4(e)(1) through (4).
- Oversee my organization's service providers by meeting the requirements of 16 C.F.R. §314.4(f)(1) through (3).
- Evaluate and adjust my organization's information security program in light of the results of the required testing and monitoring required by 16 C.F.R. §314.4(d); any material changes to my organization's operations or business arrangements; the results of the required risk assessments under 16 C.F.R. §314.4(b)(2); or any other circumstances that I know or have reason to know may have a material impact on my organization's information security program as required by 16 C.F.R. §314.4(g).
- Establish an incident response plan that meets the requirements of 16 C.F.R. §314.4(h).
- Require my organization's Qualified Individual to report regularly and least annually to those with control over my organization on my organization's information security program as required by the 'Safeguards Rule' under 16 C.F.R. §314.4(i).

My signature below affirms that I have read these responsibilities and agree to abide by them.

Box 1 Authorizing Official First and Last Name_____

Authorizing Official Title _____

Signature _____ Date_____

Paperwork Burden Statement

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless such collection displays a valid OMB control number. The valid OMB control number for this information collection is 1845-NEW. Public reporting burden for this collection of information is estimated to average 10-20 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. The obligation to respond to this collection is required to obtain or retain a benefit (20 U.S.C. 1070 *et seq.*). If you have comments or concerns regarding the status of your individual submission of this application, please contact the **FSA Partner and School Relations Center** via the Contact Customer Support form on FSA Partner Connect (https://fsapartners.ed.gov/help-center/contact-customer-support) or phone at 1-800-848-0978 (Monday through Friday, 8:00 A.M. to 8:00 P.M. Eastern Time) directly.