INSTRUCTIONS:

To designate a different person to sign your SAIG Enrollment documents, complete the information on the Designation of Authorizing Official form and have the President or CEO on file with ED sign the form.

Certification of the President/CEO or Designee

The U.S. Department of Education is required to collect the signature of the chief officer of the organization (President or CEO that is currently on file with ED) for assigning a designee.

The original signature document must be submitted to CPS/SAIG Technical Support. CPS/SAIG Technical Support cannot accept stamped, photocopied, or electronically signed signatures. Signatures must be original if mailed to CPS/SAIG Technical Support

A copy of each signed and dated statement must be maintained by your organization.

Sending Designee Signature Pages

Completed and signed designee pages can be e-mailed, faxed, or mailed to CPS/SAIG Technical Support.

E-mail: cpssaig@ed.gov

Fax: 319-665-7662

Mail:

CPS/SAIG Technical Support
2450 Oakdale Blvd., Second Floor
Coralville, IA 52241-9728

PLEASE NOTE: Your enrollment request will not be processed until CPS/SAIG Technical Support receives all certification statements, completed, and signed.

Designation of Authorizing Official

Current Designee: _____

If you as the President or CEO wish to designate someone other than yourself to sign SAIG enrollment applications, you may do so by completing the designation statement below and signing Box 1. Have your designee complete and sign Box 2.

I hereby designate_____with the title_____, to be my
(Name of New Designee - Required) (Position Title of New Designee - Required)
responsible authorizing official for all future Federal Student Aid System enrollment applications. All related responsibilities of the President/CEO shall be carried out by this designee. As President/CEO, I agree to assume the responsibility for such actions associated with this and future enrollment agreements. This designation is effective as of the date signed below.

Note: Authorized Official name and signature must match information on file with ED.

Box 1 SAIG Customer Name (Required):_____
_____

President/CEO_____Title_____
_____
(Printed name of President/CEO – Required) (Position title – Required)

Signature_____Date_____

Responsibilities of the President/CEO or Designee

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

- I or my designee will notify CPS/SAIG Technical Support within one business day, by e-mail at CPSSAIG@ed.gov or call 1-800-330-5947 when any person no longer serves as a designated authorizing official, Primary DPA, or Non-Primary DPA.
- I will not permit unauthorized use or sharing of SAIG passwords or codes that have been issued to anyone at my organization.
- Each person who is a SAIG DPA for my organization has read and signed a copy of "Step Three: Responsibilities of the Primary and Non-Primary Destination Point Administrator."
- Each person who is a SAIG DPA for my organization has made a copy of the signed Step Three document for his or her own files and a copy is maintained at my organization.
- My organization has provided security due diligence and verifies that administrative, operational, and technical security controls are in place and are operating as intended. Additionally, my organization verifies that it performs appropriate due diligence to ensure that, at a minimum, any employee who has access to Federal Student Aid (FSA) ISIR data meets applicable state security requirements for personnel handling sensitive personally identifiable information.
- 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 as stated in 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 DPA or the Qualified Individual identified under 16 C.F.R. Part 314 must notify Federal Student Aid at CPSSAIG@ed.gov within 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 have signed this certification below and sent the original to the Department. I have retained a copy of this certification at the organization. My signature below affirms that I have read these responsibilities and agree to abide by them.
- I have ensured that the Standards for Safeguarding Customer Information (as the term customer information applies to my institution – See Glossary), 16 C.F.R. Part 314, issued by the Federal Trade Commission (FTC), as required by the Gramm-Leach-Bliley (GLB) Act, 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 GLB Act 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, HEA 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 institution's information security program and enforcing my institution's information security program in compliance with 16 C.F.R. 314.4(a).

- Base my institution'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 institution – See Glossary) 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 institution 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 institution 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 institution's information security program and meet the requirements of 16 C.F.R. 314.4(e)(1) through (4).
- Oversee my institution's service providers (See Glossary) by meeting the requirements of 16 C.F.R. 314.4(f)(1) through (3).
- Evaluate and adjust my institution'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 institution'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 institution'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 institution's Qualified Individual to report regularly and least annually to those with control over my institution on my institution's information security program as required by 16 C.F.R. 314.4(i).

Box 2 New Designee_____Title _____
(Printed name of the New Designee – Required) (Position title – Required)

Signature_____Date _____
(Original signature must be submitted. Stamped or electronic signatures will not be accepted. – Required)

Name of School or Agency (Required): _____

Office Use Only

Customer Number_____

TG Number_____