# Data Security Operating Policy (DSOP)

**Employer-Funded Financial Aid (EFFA)**

## Table of Contents

*This document contains sensitive, confidential, and trade secret information, and must not be disclosed to third parties without the express prior written consent of Employer-Funded Financial Aid (EFFA).*

## Section 1: Introduction to DSOP and Standards for Protection

As a leader in financial aid administration and payment processing, EFFA has a commitment to protect Student Payment Data and Sensitive Authentication Data, ensuring that it is kept secure.

Compromised data negatively impacts employees, students, Partners, Service Providers, and financial institutions. Even one incident can severely damage a company's reputation and impair its ability to effectively conduct business. Addressing this threat by implementing security operating policies can help improve customer trust, increase profitability, and enhance a company's reputation.

EFFA knows that our Partners and Service Providers (collectively, you) share our concern and requires, as part of your responsibilities, that you comply with the data security provisions in your agreement to process financial aid payments and related services (the Agreement) and this Data Security Operating Policy (DSOP), which we may amend from time to time. These requirements apply to all your equipment, systems, and networks (and their components) on which Encryption keys, Student Payment Data, or Sensitive Authentication Data (or a combination of those) are stored, processed, or transmitted.

Capitalized terms used but not defined herein have the meanings ascribed to them in the glossary at the end of this policy.

The Data Security Operating Policy (DSOP) is a set of comprehensive policy requirements designed to protect Account Data whenever such data is stored, processed, or transmitted.

EFFA requires all Partners and Service Providers to be SOC-2 compliant. As part of that requirement, you must, and you must cause your Covered Parties to:

- Store Student Payment Data only to facilitate EFFA financial aid transactions in accordance with, and as required by, the Agreement.

- Comply with current SOC-2 requirements and other applicable data security standards related to your processing, storing, or transmitting of Encryption Keys, Student Payment Data, or Sensitive Authentication Data.

- Ensure industry-approved security products and practices are used when deploying or replacing technology to store, process, or transmit data.

You must protect all EFFA payment records and financial aid records retained pursuant to the Agreement in accordance with industry standard data security provisions; you must use these records only for purposes of the Agreement and safeguard them accordingly. You are financially and otherwise liable to EFFA for ensuring your Covered Parties' compliance with these data security provisions.

## Section 2: Data Incident Management Obligations

You must notify EFFA immediately and in no case later than seventy-two (72) hours after discovery of a Data Incident.

To notify EFFA, contact the EFFA Enterprise Incident Response Program (EIRP) by email at EIRP@effa.com. You must designate an individual as your contact regarding such Data Incident. In addition:

- You must conduct a thorough investigation of each Data Incident and promptly provide to EFFA all Compromised Account Numbers. EFFA reserves the right to conduct its own internal analysis to identify data involved in the Data Incident.

**For Data Incidents involving fewer than 10,000 unique Account Numbers:** An investigation summary must be provided to EFFA within ten (10) business days of its completion.

**For Data Incidents involving 10,000 or more unique Account Numbers:** You must engage a qualified cybersecurity forensic investigator to conduct this investigation within five (5) days following discovery of a Data Incident. The unedited forensic investigation report must be provided to EFFA within ten (10) business days of its completion.

- Investigation summaries should contain the following information: incident summary, description of the affected environment(s), timeline of events, key dates, impact and data exposure details, containment and remediation actions, and attestation there is no indication additional EFFA data is at-risk.

- Forensic investigation reports must include forensic reviews, compliance assessments, and all other information related to the Data Incident; identify the cause of the Data Incident; confirm whether or not you were in compliance with applicable data security standards at the time of the Data Incident; and verify your ability to prevent future Data Incidents by providing a plan for remediating all security deficiencies.

Notwithstanding the foregoing paragraphs of this Section 2, "Data Incident Management Obligations":

- EFFA may, in its sole discretion, require you to engage a qualified forensic investigator to conduct an investigation of a Data Incident for Data Incidents involving fewer than 10,000 unique Account Numbers or where multiple incidents have occurred within a 12-month period. Any such investigation must comply with the requirements set forth above in this Section 2, "Data Incident Management Obligations" and must be completed within the timeframe required by EFFA.

- EFFA may, in its sole discretion, separately engage a qualified forensic investigator to conduct an investigation for any Data Incident and may charge the cost of such investigation to you.

You must assess the Data Incident under applicable data breach notification laws globally and, where deemed necessary, notify applicable regulators and impacted individuals in accordance with such data breach notification laws. If you have determined that your Service Provider or another entity is responsible for reporting the Data Incident, you shall advise such Service Provider or entity of its duty to assess its reporting obligations under applicable data breach notification laws. You agree to obtain written approval from EFFA prior to referencing or naming EFFA in any communications to individuals about the Data Incident.

You agree to work with EFFA to provide details and rectify any issues arising from the Data Incident, including providing (and obtaining any waivers necessary to provide) to EFFA all relevant information to verify your ability to prevent future Data Incidents in a manner consistent with the Agreement.

Notwithstanding any contrary confidentiality obligation in the Agreement, EFFA has the right to disclose information about any Data Incident to affected individuals, financial institutions, other participants on payment networks, and the general public as required by Applicable Law; by judicial, administrative, or regulatory order, decree, subpoena, request, or other process; in order to mitigate the risk of fraud or other harm; or otherwise to the extent appropriate to operate EFFA's financial aid network.

### What to do if you have a Data Incident?

Please follow these steps if you have identified a Data Incident at your business.

**Step 1:** Fill out the Partner Data Incident Initial Notice Form and email to EIRP@effa.com within 72 hours after the Data Incident is discovered.

**Step 2:** Conduct a thorough investigation; this may require you to hire a qualified cybersecurity forensic investigator.

**Step 3:** Promptly provide us with all compromised EFFA account numbers.

**Step 4:** Work with us to help resolve any issues arising from the Data Incident.

View Section 2, "Data Incident Management Obligations" for more details on Data Incident Management Obligations.

### Have more questions?

Contact: EIRP@effa.com

## Section 3: Indemnity Obligations for a Data Incident

Your indemnity obligations to EFFA under the Agreement for Data Incidents shall be determined, without waiving any of EFFA's other rights and remedies, under this Section 3, "Indemnity Obligations for a Data Incident". In addition to your indemnity obligations (if any), you may be subject to a Data Incident non-compliance fee as described below in this Section 3, "Indemnity Obligations for a Data Incident".

You may be required to compensate EFFA for Data Incidents that involve:

- 10,000 or more EFFA Account Numbers with either of the following:
  - Sensitive Authentication Data, or
  - Account expiration information

However, EFFA will not seek indemnification from you for a Data Incident that involves:

• fewer than 10,000 EFFA Account Numbers, or • more than 10,000 EFFA Account Numbers, if you meet the following conditions:

- you notified EFFA of the Data Incident pursuant to Section 2, "Data Incident Management Obligations",
- you were in compliance at the time of the Data Incident with applicable data security standards (as determined by the forensic investigator's investigation of the Data Incident), and
- the Data Incident was not caused by your wrongful conduct or that of your Covered Parties.

Notwithstanding the foregoing paragraphs of this Section 3, "Indemnity Obligations for a Data Incident", for any Data Incident, regardless of the number of EFFA Account Numbers, you shall pay EFFA a Data Incident non-compliance fee not to exceed USD $100,000 per Data Incident (as determined by EFFA in its sole discretion) in the event that you fail to comply with any of your obligations set forth in Section 2, "Data Incident Management Obligations". For the avoidance of doubt, the total Data Incident non-compliance fee assessed for any single Data Incident shall not exceed USD $100,000.

EFFA will exclude from its calculation any EFFA Account Number that was involved in a prior Data Incident indemnity claim made within the twelve (12) months prior to the Notification Date. All calculations made by EFFA under this methodology are final.

EFFA may bill you for the full amount of your indemnity obligations for Data Incidents or deduct the amount from EFFA's payments to you (or debit your Bank Account accordingly) pursuant to the Agreement.

Your indemnity obligations for Data Incidents hereunder shall not be considered incidental, indirect, speculative, consequential, special, punitive, or exemplary damages under the Agreement; provided that such obligations do not include damages related to or in the nature of lost profits or revenues, loss of goodwill, or loss of business opportunities.

In its sole discretion, EFFA may reduce the indemnity obligation for Partners solely for Data Incidents that meet each of the following criteria:

• Applicable Risk-Mitigating Technologies were used prior to the Data Incident and were in use during the entire Data Incident Event Window, • A thorough investigation in accordance with industry standards was completed (unless otherwise previously agreed in writing), • Forensic report clearly states the Risk-Mitigating Technologies were used to process, store, and/or transmit the data at the time of the Data Incident, and • You do not store (and did not store throughout the Data Incident Event Window) Sensitive Authentication Data or any Student Payment Data that has not been properly encrypted or secured.

Where an indemnity reduction is available, the reduction to your indemnity obligation (excluding any non-compliance fees payable) shall be determined based on the effectiveness of security measures implemented, with reductions ranging from 25% to 75% as determined by EFFA based on the forensic investigation findings.

## Section 4: Targeted Analysis Program (TAP)

Student Payment Data compromises may be caused by data security gaps in your Student Payment Data Environment (SPDE).

Examples of Student Payment Data compromise include, but are not limited to:

• **Common Point of Purchase (CPP):** EFFA participants report fraudulent Transactions on their accounts and are identified and determined to have originated from making transactions at your locations.

• **Payment Data found:** EFFA student payment and account data found on the world wide web linked to Transactions at your locations.

• **Malware suspected:** EFFA suspects you are using software infected with or vulnerable to malicious code.

TAP is designed to identify potential Student Payment Data compromises.

You must, and you must cause your Covered Parties to, comply with the following requirements upon notification from EFFA of a potential Student Payment Data compromise:

• You must promptly review your SPDE for data security gaps and remediate any findings.

- You must cause your third-party vendor(s) to conduct a thorough investigation of your SPDE if outsourced.

• You must provide a summary of action taken or planned after your review, evaluation and/or remediation efforts upon notification from EFFA.

• You must provide updated data security validation documents in accordance with your SOC-2 compliance requirements.

• As applicable, you must engage a qualified cybersecurity forensic investigator to examine your SPDE if you or your Covered Party:

- Cannot resolve the Student Payment Data compromise within a reasonable period of time, as determined by EFFA, or
- Confirm that a Data Incident has occurred and comply with the requirements set forth in Section 2, "Data Incident Management Obligations".

If your TAP obligations are not satisfied, then EFFA has the right to impose non-compliance fees, withhold payments, and/or terminate the Agreement.

## Section 5: Confidentiality

EFFA shall take reasonable measures to keep (and cause its agents and subcontractors to keep) your security assessment reports, including any Validation Documentation in confidence and not disclose such documentation to any third party (other than EFFA's Affiliates, agents, representatives, Service Providers, and subcontractors) for a period of three years from the date of receipt, except that this confidentiality obligation does not apply to documentation that:

a. is already known to EFFA prior to disclosure; b. is or becomes available to the public through no breach of this paragraph by EFFA; c. is rightfully received from a third party by EFFA without a duty of confidentiality; d. is independently developed by EFFA; or e. is required to be disclosed by an order of a court, administrative agency or governmental authority, or by any law, rule or regulation, or by subpoena, discovery request, summons, or other administrative or legal process, or by any formal or informal inquiry or investigation by any government agency or authority (including any regulator, inspector, examiner, or law enforcement agency).

## Section 6: Disclaimer

EFFA HEREBY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES, AND LIABILITIES WITH RESPECT TO THIS DATA SECURITY OPERATING POLICY, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FINANCIAL INSTITUTIONS ARE NOT THIRD PARTY BENEFICIARIES UNDER THIS POLICY.

## Section 7: Glossary

For purposes of this Data Security Operating Policy only, the following definitions apply and control:

**Account Data** consists of Student Payment Data and/or Sensitive Authentication Data. See Student Payment Data and Sensitive Authentication Data.

**Account Holder** means a student or employee to whom a payment account is issued, or any individual authorized to use the payment account for educational expenses.

**Account Information** means information about EFFA participants and payment transactions, including names, addresses, account numbers, and account identification numbers.

**Account Number** means the unique identifying number that EFFA assigns to the account when it is issued.

**Agreement** means the General Provisions, the Partner Regulations, and any accompanying schedules and exhibits, collectively (sometimes referred to as the EFFA Partnership Agreement in our materials).

**Compromised Account Number** means an EFFA account number related to a Data Incident.

**Consumer** is defined as an account holder purchasing learning-related services through EFFA's platform.

**Covered Parties** means any or all of your employees, agents, representatives, subcontractors, Processors, Service Providers, providers of your point-of-sale (POS) equipment or systems or payment processing solutions, Entities associated with your EFFA Partner account, and any other party to whom you may provide Student Payment Data or Sensitive Authentication Data (or both) access in accordance with the Agreement.

**Data Incident** means an incident involving the compromise or suspected compromise of EFFA encryption keys, or at least one EFFA account number in which there is:

- unauthorized access or use of Encryption Keys, Student Payment Data, or Sensitive Authentication Data (or a combination of each) that are stored, processed, or transmitted on your equipment, systems, and/or networks (or the components thereof) of yours or the use of which you mandate or provide or make available;
- use of such Encryption Keys, Student Payment Data, or Sensitive Authentication Data (or a combination of each) other than in accordance with the Agreement; and/or
- suspected or confirmed loss, theft, or misappropriation by any means of any media, materials, records, or information containing such Encryption Keys, Student Payment Data, or Sensitive Authentication Data (a combination of each).

**Data Incident Event Window** means the window of intrusion (or similarly determined period of time) set forth in the final forensic report, or if unknown, up to 365 days prior to the last Notification Date of potentially Compromised Account Numbers involved in a Data Incident reported to us.

**Encryption Key** (EFFA encryption key) means all keys used in the processing, generation, loading, and/or protection of account data. This includes, but is not limited to, data encryption keys, access control keys, and authentication keys used to secure Student Payment Data.

**Notification Date** means the date that EFFA provides financial institutions with final notification of a Data Incident. Such date is contingent upon EFFA's receipt of the final forensic report or internal analysis and shall be determined in EFFA's sole discretion.

**Partner** means the Partner and all of its affiliates that process financial aid payments under an Agreement with EFFA or its affiliates.

**Partner Level** means the designation we assign Partners related to their data security compliance validation obligations, based on transaction volume and risk assessment.

**Point of Sale (POS) System** means an information processing system or equipment, including a terminal, personal computer, contactless reader, or payment engine or process, used by a Partner to obtain authorizations or to collect Transaction data, or both.

**Primary Account Number** means the unique payment account identifier assigned to each EFFA account.

**Processor** means a service provider to Partners who facilitate authorization and submission processing to the EFFA network.

**Risk-Mitigating Technology** means technology solutions that improve the security of EFFA Student Payment Data and Sensitive Authentication Data, as determined by EFFA. To qualify as a Risk-Mitigating Technology, you must demonstrate effective utilization of the technology in accordance with its design and intended purpose. Examples include, but may not be limited to: end-to-end encryption, tokenization, and multi-factor authentication.

**Sensitive Authentication Data** means security-related information used to authenticate account holders and/or authorize payment transactions. This information includes, but is not limited to, account verification codes, authentication tokens, PINs, and PIN blocks.

**Service Providers** means authorized processors, third party processors, gateway providers, integrators of POS systems, and any other providers to Partners of POS systems, or other payment processing solutions or services.

**Student Payment Data** means at a minimum, the full Primary Account Number by itself or full Primary Account Number plus any of the following: account holder name, expiration date, and/or service code. See Sensitive Authentication Data for additional data elements that might be transmitted or processed (but not stored) as part of a payment transaction.

**Student Payment Data Environment (SPDE)** means the people, processes, and technology that store, process, or transmit Student Payment Data or Sensitive Authentication Data.

**Targeted Analysis Program (TAP)** means a program that provides early identification of a potential Student Payment Data compromise in your Student Payment Data Environment (SPDE). See Section 4, "Targeted Analysis Program (TAP)".

**Transaction** means a payment, credit, cash advance (or other cash access), or financial aid disbursement completed through EFFA's system.

**Transaction Data** means all information required by EFFA, evidencing one or more Transactions, including information obtained at the point of transaction, information obtained or generated during authorization and submission, and any dispute information.

**Transaction Record** means a reproducible (both paper and electronic) record of a Transaction that complies with our requirements and contains the Account Number, Transaction date, dollar amount, authorization, account holder signature (if applicable), and other information.

**Validation Documentation** means security assessment reports, compliance attestations, vulnerability scan summaries, and other documentation demonstrating adherence to applicable data security standards.

*This document contains sensitive, confidential, and trade secret information, and must not be disclosed to third parties without the express prior written consent of Employer-Funded Financial Aid (EFFA).*

**Document Version:** April 2025
**Contact:** EFFAPCIComplianceProgram@effa.com