Policy IT1.01: Information Security

Oversight	Information
Policy Type	Information Technology
Policy Owners	Chief Information Officer
Initial Policy Approval Date	March 6, 2019
Current Revision Approval Date	June 8, 2020
Procedure Effective Date	June 8, 2020

Policy

American Sentinel University takes the protection of our student's secure information very seriously. Failure to adhere to the guidelines contained in this policy may lead to termination of employment and/or legal implications. While the university cannot fully guarantee privacy of electronic information, files may be examined by administrative personnel to determine if any users, student or employee, are acting in violation of these policies. We will ensure privacy through the following:

- American Sentinel will not release, sell, rent, or trade your personal information gathered on the website to any third party for the promotion of other services or products.

All employees will adhere to privacy guidelines and keep data secure through the policies listed and student identity verification in compliance with the United States Federal Higher Education Opportunity Act (HEOA) of 2008,

- Public Law 110-315.
- Data access is only authorized to employees and third parties who need the information to perform their associated duties.
- The university information security 'program' is coordinated by the Senior Systems Administrator

Sensitive data access is controlled by strict permissions by department and is controlled by individual login accounts as deemed appropriate.

Data Security

The person assigned university owned computing hardware assumes full responsibility for the safekeeping of both the hardware and software. Upon termination of faculty or staff, the HR Department or designee will initiate network access account termination with IT within 24 hours. Non-administrative data is owned by the department or project that creates and maintains the data or the person (faculty, staff, or enrolled student) assigned to the login associated with the data. In the event the data owner is no longer enrolled or employed at American Sentinel University, the data owner or Department Head must provide explicit authorization for other

persons to access the data. The administrative department having primary responsibility for creation and maintenance of the data content owns administrative data.

American Sentinel's applications and databases are protected by hardware and software firewalls. In addition, the University employs Secure Socket Layer (SSL) encryption technology for data transmission.

Collection

American Sentinel automatically collects anonymous statistical data about the use of its website (browser, Internet domain, computer operating system and IP address and navigation path for visitors to the website). We may also collect personal data including, but not limited to names, addresses, emails, or other information that is voluntarily submitted by visitors and prospective students.

The American Sentinel website uses the first-party Google Analytics. This site also uses the third-party cookies to enable reporting on demographics and interests information (such as age, gender, and favored product categories), but, again, not in any way that is associated with personally identifiable information.

As students navigate through and interact with Our Platform, American Sentinel may use automatic data collection technologies to collect certain information about equipment, browsing actions, and patterns. This includes traffic and location data, logs, IP address, operating system, browser type, and other communication and resources accessed on the website.

American Sentinel does not knowingly collect personal data from children under the age of 13 through our website.

Usage

The university does not use or exploit information and data. American Sentinel uses data to improve the navigation, functionality and content of its website and to improve its program and services. Personal data and data collected through cookies is used to:

- Communicate with students to provide them requested information and to tell them about our program and services.
- Help university officials make informed admission decisions.
- Verify students' identities prior to granting access to certain American Sentinel services and resources.
- Communicate with individuals once they become students.
- To present and maintain the website platform to improve navigation, functionality, and operability.
- To contact students with newsletters or promotional, advertising, or marketing materials.
- To contact students in regard to change in policy
- To provide notifications of account changes, expiration and renewal notices.

- Carry out any obligations and enforce rights arising from contracts between the student and university.
- Monitor, observe, or examine use and access of university platforms.
- Enable students to use and activate interactive features on the website.
- Provide students with information, contents, resources, products, and services related to students.

Sharing

American Sentinel University does not disclose, release, sell, or trade information and data of students to third-party persons and entities. American Sentinel may disclose aggregated information and data, including personal data, of students, only insofar as the information is deidentified. We may disclose student information and data:

- To our subsidiaries, affiliates, successors, and assignees
- To contractors, Service Providers (as defined later herein), learning resources, assessment sites, external vendors, and other third parties
- To a buyer or any successor in interest in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of the university assets.
- To fulfill the purpose for which the student provides such information
- To provide students with a quality learning experience
- To comply with any court order, law, or legal process, including to respond to any government or regulatory request
- Where such disclosure is necessary or appropriate to protect the rights, property, or safety of university, students, any third parties, or others, including the exchange of information with other entities for the purposes of fraud protection and credit-risk reduction
- To protect and maintain the security, operability, viability, functionality, and reliability of the university sites
- To prevent or investigate potential, threatened, potential, or actual wrongdoing
- For all other grounds, contingent upon student consent.

These companies, organizations and individuals may need this information to perform their functions. They are not authorized to use the information we share with them for any other purpose. Occasionally, American Sentinel may send information about products and services we think may be of interest to students. Sometimes American Sentinel may share this information with its educational partners to bring similar information to students' attention.

Third-party entities (including Google Analytics and DoubleClick Digital Marketing), individuals, contractors, and/or subcontractors employed to facilitate in the activities of the university may only use, access or disclose student information for the sole purpose of performing facilitative services.

Storage

American Sentinel will retain collected data, including personal data, only for as long as is necessary for the purposes set out in this policy. Information will be retained to the extent necessary to comply with legal obligations, to resolve disputes, and to enforce legal agreements and policies.

Network drive space is a resource provided for the sole purpose of storing current work-related data. Users should, on a regular basis, review the contents of their drives and delete any files that are unnecessary. There are currently no storage limitations for specific courses or employee allocations. The course site, Moodle, does have an overall limitation and courses over 500MB can cause significant performance issues when backing up or restoring on production servers. Typically, student course work related to discussion forums and / or assignments have a 20MB or less limitation in place at the course level.

Student information, including Personal Data, may be transferred to, and maintained on, devices located outside of the students' state, province, country, or other governmental jurisdiction where the data protection laws may differ. American Sentinel University shall take reasonable measures to ensure that student data is treated securely and in accordance with this policy, and that no transfer of student data to a third-party organization or a country shall occur, unless there are adequate controls in place regarding data privacy, including personal data, and the information security protocol. Students located outside of the United States using, accessing, or visiting the university platform consent to this data transfer.

Privacy of electronic information

Administrative rights and access to certain information will only to be given to specific employees as needed to fulfill their responsibilities at the university. The university reserves the right to limit or restrict any individual's use of any resource, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine security, integrity, or the effective operation of the university's computing and communications facilities and/or which are in violation of this policy.

Protected Academic Records (PAR) and Personal Identifying Information (PII), must be encrypted when shared in the following situations:

Examples of when encryption is required include, but are not limited to:

- A University employee, student, contractor, or vendor sending or receiving the PAR or PII using his/her home's Internet Service Provider (ISP) connection unless both (a) over a Virtual Private Network (VPN) connection, and (b) transmitting only to a destination within the campus network.
- Any transmission of PAR or PII sent over any off-campus network, unless both (a) using a VPN connection, and (b) transmitting only to a destination within the campus network.

Use of the campus wireless network does not require VPN as long as one is transmitting to a destination within the campus.
- Any vendor transmissions of PAR or PII sent over the Internet.
- Use of a cellular or mobile network transmit student information.

Encryption is not required for a University employee who uses an on-campus workstation with a wired connection to the University network to transmit a document to another in-house employee or to save a document containing PAR or PII to his/her University-managed network folder.

California Consumer Privacy Act

To the extent the Company is governed by the CCPA (please below in section titled "Rights under the California Consumer Privacy Act ("CCPA")," Company shall provide the User with a clear and conspicuous link, titled "Do Not Sell My Personal Information," wherein such link will direct the User to a webpage on the Platform that enables the User to opt-out of the sale of the User's Personal Data.

To the extent the university performs, operates, or executes business in the State of California, and meets any of the following three (3) criteria, the university is subject to the obligations and mandates of the CCPA:

- Has gross annual revenues in excess of $25 million;
- On an annual basis, buys, receives, or sells the personal information of at least 50,000 California consumers, households, or devices; or
- Derives at least fifty percent (50%) of its annual revenue from the sale of California consumers' personal information.

To the extent the university is subject to the obligations and mandates of the CCPA, the student shall be awarded the following rights:

- The right to know what personal information is collected, used, shared, or sold both as to the categories and specific pieces of personal information;
- The right to delete personal information held by the university and by extension, the Service Providers;
- The right to opt-out of sale of personal information, including Personal Data;
- The right to non-discrimination in terms of price, service, access, use, or consumption of resources, including the Website, when the student exercises a privacy right available under the CCPA; and
- All other obligations and mandates available under the CCPA, available at Cal. Civ. Code § 1798.100 *et seq*, effective as of January 1, 2020.

General Data Protection Regulation

American Sentinel University shall be subject to the General Data Protection Regulation if it has an establishment in the European Union, offers goods and services to residents of the European Union, or monitors the behavior of residents in the European Union. The regulations give students the following rights under Chapter 3.

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure or deletion
- The right to restrict processing
- The right to portability or personal information
- The right to object
- Rights in relation to automated decision making and profiling.

Opt-Out Policy

Students shall receive newsletters, marketing or promotional materials, and other communications that American Sentinel University deems would be of interest to the Students. Students may expressly opt out of receiving any, or all, of these communications from the university.

Guidelines

- Not Applicable

Procedure

Electronic Media

Overwriting Hard Drives for Sanitization: Overwriting is an approved method for sanitization of hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented. Overwriting consists of recording data onto magnetic media by writing a pattern of fluxes or pole changes that represent binary ones (1) and zeroes (0). These patterns can then be read back and interpreted as individual bits, 8 of which are used to represent a byte or character. If the data is properly overwritten with a pattern (e.g., “11111111″ followed by “00000000″) the magnetic fluxes will be physically changed, and the drives read/write heads will only detect the new pattern and the previous data will be effectively erased. To purge the hard drive requires overwriting with a pattern, and then its complement, and finally with another pattern (e.g., overwrite first with “00110101 “, followed by “11001010″, then “10010111″). Sanitization is not

complete until the third overwrite passes and a verification pass are completed. A variety of software packages are available on the open market that properly perform this function. Examples of software programs that can be used to overwrite media include Pretty Good Privacy, Eraser, and KillDisk.

Disposal of Hard Drives:
Transfer of Hard Drives to Other Departments or Outside of American Sentinel University. Prior to transfer, operable hard drives must be overwritten in accordance with the procedures in "Overwriting Hard Drives for Sanitization" above. Departments should maintain documentation of proper sanitization for hard drives. Equipment designated for surplus or other re-use should have a label affixed stating that the hard drive has been properly sanitized.

Transfer of Hard Drives within a Department:
Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. All electronic media should be sanitized per "Overwriting Hard Drives for Sanitization" above, however; because the drive is remaining within the department, the hard drive may instead be formatted prior to transfer. Insofar as special recovery tools would have to be used by an individual to access the data erased by this method, any attempt by an individual to access unauthorized data would be viewed as a conscious violation of state or federal regulations and the American Sentinel University Confidentiality Statement.

Sending a Hard Drive Out for Repair or for Data Recovery:

The vendor repairing or recovering data on the hard drive must sign an appropriate agreement with the University, ensuring that the vendor will take proper care of the data. Once data is recovered or the hard drive is repaired, the original hard drive must be returned to the owner so that the owner can then handle it as per this American Sentinel University policy for proper disposal of hard drives.

Disposal of Damaged or Inoperable Hard Drives:

The owner must first attempt to overwrite the hard drive in accordance with the procedures in paragraph A1 above. If the hard drive cannot be overwritten, the hard drive must be disassembled and mechanically damaged so that it is not usable by a computer. It is recommended that a hard-drive shredding service be used to ensure mechanical damage to the hard drive so that it is no longer useable

Detachable Media:

The transfer of personal and sensitive information on detachable such as USB and external hard drives is strictly prohibited.

Related Documents/References

- Student and FERPA policy
- Faculty and FERPA policy
- Federal Higher Education Opportunity Act (HEOA) of 2008, Public Law 110-315

Definitions

- ***Protected Academic Records (PAR):*** *University administrative computer data:* employee personnel records, student education records, university financial information, and electronic documents that contain confidential information.
- ***Personal Identifying Information (PII):*** includes any information that can be used to identify you or another person, including:
    - *Personal information:* social security numbers, driver's license numbers, etc.
    - *Financial information:* bank account numbers, credit card numbers, etc.
    - *Passwords:* of university systems or personal accounts on non-university systems.

Revision History

- October 2018 – Consolidated AA6.15 Privacy, AA9.02 Student Identification Verification, IT1.01 Information Security Policy, IT01.11 Privacy of Electronic Information, IT1.04 Data Storage, and IT1.04 Transmission of Private Information.
- January 14, 2020 – Remove info on student identification verification, consolidated IT1.07 standards for electronic media, and added senior systems administrator as the policy owner.
- May 7, 2020: Updated policy format for accessibility guidelines - AHB
- June 8, 2020: Removed policies related to the clean desk checks as this has been added as its own policy. Added information related to the California Privacy Act - AHB