



Policy of Security, Integrity and Fraud protection

Main Topics

- ⇒ Security of examination material
- ⇒ Guidelines of Physical security
- ⇒ Security of Computers used to prepare Examination Materials
- ⇒ Use of Supported Machines
- ⇒ Protecting confidential data/Securely sharing /Encrypting
- ⇒ Sensitive Data Handling Procedures
- ⇒ Credit Card Data Retention Policy

Appendix

- ⇒ Confidentiality Statement to all employees
- ⇒ Exam Paper Register Form



Security of examination material and protection of personal/confidential data

Secure storage of exam materials and with together this, the protection of personal and priority datas are very important which are also governed by the PSA's Data Protection Policy as well as governed by the new European union regulation (the General Data Protection Regulation (GDPR)) which is 25 May 2018 will enter into force.

Therefore the **EU General Data Protection Regulation (GDPR)** replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. for more information the new regulation and policies: <https://www.eugdpr.org/eugdpr.org.html> - what also will applies by PSA.

As the PSA Educational Centres begin to receive exam materials and personal data from the awarding organisations and future candidates, the issue of secure storage and data protection, becomes one very important but which primarily concerns PSA exams office staff.

The security of examination materials is of the utmost importance and PSA Educational and Training Department will already have procedures in place to communicate with colleagues and external examiners, as well as to store examination papers and scripts during the assessment process.

The PSA International Group™/PSA Academy™ Standing Committee on Assessment would like to remind departments of the need for vigilance and to encourage Education and Training Departments and faculties to undertake regular reviews of their processes.

General points

The PSA Academy™ has been registered and government-approved on several continents and in several countries as an a Independent Private Adult Educational Institute and Academy, - therefore it also has to comply with several national and international requirements for protect and storage of data and exam materials.

The Information Security Officer at the PSA in the Information Department, has developed a security policy for exam paper production which is in the Security of Computers tab. The policy should be communicated to all staff each year before they begin production of examination papers.

If there is a very remote possibility that draft or final examination papers might have been seen by unauthorised people it may be necessary to re-set the paper. Before doing so, departments should consult with the Chair of the Standing Committee on Assessment to establish whether it is necessary or whether small changes could be made to core sections of the paper that could identify academic misconduct.

Departments should ensure that new and temporary academic and administrative staff are briefed fully during the induction process about the department's procedures for the security and delivery of examination papers and material.



Security, integrity and fraud protection

Exam quality, integrity and security are critical to educational institutions when processing admissions from international students.

Our robust and comprehensive approach covers all areas – from the different test/exam material development, delivery and results processing, through to post-examination review and evaluation as well as the storage.

All the development and production processes of the exam, as well as the post-test marking and administration, are managed and controlled centrally in PSA Academy™. This means you can trust the results as a valid and accurate reflection of a candidate's ability.

1. Security of test material

All our security measures are designed to ensure that candidates cannot receive prior knowledge of the content of test/exam materials.

Test paper production

In generally the exam materials we get from that various awarding organizations. - or Tasks and items are selected from a secure electronic item bank and unique papers are constructed for each test sitting. The item bank is refreshed continuously with new material.

Test questions for the item bank are commissioned from our teams of expert test item writers. The item writers have extensive experience in the fields of the various vocational education and in the production of exam materials development.

All of them work in accordance with strict guidelines governing the type of content that is suitable for a global audience of test takers and conforms to the required quality standards.

Secure storage and despatch of materials

All confidential test materials are printed and stored within our own high-security premises and test materials are despatched securely to authorised exam and/or satellite centres by courier.

Secure storage of test material by the centre

Centres must adhere to strict requirements for the storage and transport of material.

Note: *The PSA Academy™-HQ Centre is working inside the specially armed protected government building which are a Police Station and Police Vocational School-NCO training Center of the Hungarian Government.*

The entry just restricted and under control as well as just with licensed.



Security, integrity and fraud protection

Security of test material on the test day

There are strict guidelines for the handling of test material on the test day to prevent unauthorised access.

Specific security measures for computer-based tests

Our test delivery system delivers heavily encrypted assessments via the internet directly to test centres, with test materials only decrypted at the start of the test. Test material can be accessed only during a specified time window, after which it cannot be viewed inspected to make sure they can provide suitable facilities, and they are regularly inspected.

2. Security in test/exam administration

The following procedures are designed to ensure absolute security during each test session. Candidates can only take "professional" exams at one of the our authorised satellite/exam centres.

Candidate ID checks

Our authorised exam centres check each candidate's photographic ID on the day of the test. If a supervisor or invigilator is not satisfied with the identity of the candidate, they will refuse them entry.

Test day photographs

Photographs of candidates are taken on the day of their test and these can be viewed by recognising organisations through our online Results Verification Service.

Standardised testing procedures

We provide step-by-step instructions and scripts for supervisors and invigilators to ensure that test administration is standardised, secure and fair throughout all our centres. For example, packets of test papers must be opened in front of the exam candidates and completed test papers must be sealed in an envelope directly after the test finishes.

Invigilation

Supervisors and invigilators undergo character checks and receive full training in all areas of test procedure, including how to detect attempts to cheat.



Security, integrity and fraud protection

3. Security of our exam centres/place

All our authorised satellite exam centres follow a detailed code of practice which ensures the highest standards of security throughout the testing process, from registration to the recording of results.

At the official satellite centres inspected to make sure they can provide suitable facilities, and they are regularly inspected.

Centres follow strict procedures in administering PSA Academy™ exams in a fair, secure and unbiased manner.

As part of our commitment to security, we carry out:

- ⇒ pre-approval checks and inspection
- ⇒ routine inspections and checks, including unannounced inspections
- ⇒ monitoring of anomalies in performance.

4. Security in marking and issuing of results

Our post-test processes are designed to ensure absolute security in marking and rigorous checks of test results before they are released.

Preventing conflicts of interest between examiners and candidates

There are systems in place to ensure that the integrity of test results is not endangered through any conflict of interest between test markers or examiners and test candidates. Writing scripts are anonymised and allocated to examiners at random to avoid conflicts of interest.

Monitoring anomalies in performance

For some exams we carry out automatic statistical analysis after every test session prior to release of results to identify unusual patterns of scores or responses for individual candidates, or groups of candidates.

5. View of exam results

The PSA Academy™-HQ in the near future provides a free and secure online Results Verification Service that allows students to view results: http://psa-academy.org/index.php?p=results_checker



Guidelines of Physical security

- Departments should review their arrangements for the security of examination scripts and the labelling on the drawers of filing cabinets annually.
- Where possible, draft and final examination papers within departments should be kept in locked cabinets or a safe, preferably in an alarmed office, when not being worked on.
- The keys for the cabinets should not be kept in the desk adjacent to the cabinets.
- Examination papers and materials should be delivered personally to the Examinations Office and a receipt obtained. Please, **do not**, leave material at the Registry Services Reception Desk or in the Examinations Office if unattended.
- Members of staff should be reminded that examination papers or supporting material **must not** be sent in the internal post.
- Answer scripts should always be delivered by hand to destinations within the PSA Academy™, and a receipt obtained. Registered post or similar means must be used when sending material to destinations outside the Academy.
- If an examination paper is to be re-used in future years, the Examinations Office should be notified of this via the Exam Paper Cover Sheet. These papers are referred to as 'Secure' Papers and Departments should ensure that they are not uploaded to the PSA Academy™ Digital Library at the end of the academic year.
- Given physical access to a machine for long enough, it is always possible to read the data from it unless it is encrypted, even if a machine has been switched off altogether or if it has a screensaver that requires a password. Where possible, the data should be stored on a network disk (either one of the IT Service's rented file stores or similar storage offered by a department). In this way the data is physically stored elsewhere and access to the desktop machine matters much less. The other great advantage of doing this is that it should ensure that the data is backed-up.
- Electronic versions of draft and final examination papers should not be kept locally on PCs within departments. Documents must be password protected in a secure location/drive or on a disk/CD/DVD that can be locked away.
- Drafts of examination papers should be sent either by encrypted email, secure fax, memory sticks or on floppy disks/CDs/DVDs. If using e-mail, best practice would be to encrypt the data before sending it. This can be done in many ways, but the most common ways would be to use Word's option to encrypt a document, or an encrypted pdf file, or to send the document as a ZIP file and encrypt that. The recipient can be given the password to decrypt the message via a telephone or other non-computer-based method. After the first time this is done, future messages can be sent using the same password.
- Staff should be reminded that normal e-mail (and attachments) are not secure and consultations on exam questions should not be shared in this way.



Security of Computers used to prepare Examination Materials

Draft exam papers must be treated carefully to avoid compromising the security and validity of the paper before the exam. The use of computers to draw up exam papers means that careful attention must be paid to the security of the PC used to write questions or to assemble the paper and to the way drafts are stored and transferred.

The permitted methods for sharing draft exam papers are:

1. Via shared filestore, provided either by IT Services or by the department
2. Via Google Drive with a PSA Academy™ account
3. Via an encrypted USB stick
4. Via email with an encrypted document.

We strongly recommend using either method 1 or method 2.

Remember that e-mail attachments are not secure and consultations on examination questions should not be shared in this way unless the attachment is encrypted due to the risk of

- 1) interception and
- 2) accidentally sending the email to the wrong recipient.

Encryption of attachments

This part is discussed in more detail in a later chapter how to do this and which methods are acceptable.

Use of Supported Machines

Supported machines provided by IT Services will be patched and configured appropriately as part of the supported service. On a supported machine it is best to store your draft exam papers on central filestore; either your own personal area (your M or H drives) or on a shared (departmental) filestore. This ensures that the files are stored securely centrally and proper backups are taken for disaster recovery purposes.



Use of Departmental-Run Machines (Unsupported Machines)

In order to be suitably secured, operating systems must be both currently supported by the vendor in terms of patches and be capable of being secured to a suitable standard. Please check that the version of the operating system you are using meets these requirements. In particular OS X prior to version 10.11 (El Capitan) and Windows prior to Windows 7 do not meet these requirements and must not be used for exam paper production. Windows XP and Windows Vista have stopped receiving security updates from Microsoft and must not be used for the production of exam papers.

General Requirements for PCs

- Be only accessible via user accounts, and a separate account must be used for each user. "Guest" type accounts must not be used.
- Be fully patched with the vendors latest patches and kept up-to-date at all times
- Use a file system that only allows the author or owner of a file to read it

Must not export/share their hard drive or run file sharing software

Special Requirements for Windows Machines

Be fully patched via <http://update.microsoft.com>

- Set to automatically download and install patches
- Run an up-to-date virus checking software

Be scanned for spyware and adware on a regular basis

All local hard drives must be configured with the NTFS file system and not the FAT file system to ensure that only the owner of a file can read it

Must not be configured to share their C:/ drive (or other hard drives if fitted)

Google Mail/Docs

Google Mail and Docs are now the University's official platform for email and collaboration. We strongly recommend the use of Google Drive as a method of securely sharing documents. Google Drive can be used to store any sort of file (i.e. as a "cloud USB stick") and it is not necessary to use the Google word processing apps etc to use Google Drive.



Physical Security

Machines should be kept in a locked office and access to this office should be restricted. In particular, visitors or students should not have unaccompanied access to the machine. Whenever the machine is left it must be either switched off or a screensaver/screenlock must be used that requires a password to gain access. It is best to set your screensaver to lock the screen automatically after a fairly short period of inactivity (for example 5 minutes) to ensure this.

Use of Laptops

Laptops that are used both at home and on the Academy network present particular security risks. When placed on the internet or an unsecured home connection they can become infected in many ways, and then bring these problems back onto the Academy network.

To ensure security, laptops must also run a firewall and be encrypted:

Note: Encryption is discussed in more detail in a later chapter how to do this and which methods are acceptable.

[The firewall can link to <https://support.microsoft.com/en-us/help/4028544/windows-turn-windows-firewall-on-or-off>]

Use of Home Machines

Machines in the homes of members of staff should not be used for the production of exam papers unless

- They are used only by the member of staff and not by any other members of their family etc.
- The machine is secured as per the instructions for departmentally run machines above and also runs a personal firewall.

The transfer of files between home and work must be done via the WebVPN, Google Drive or (as a worst option) encrypted USB stick.

Use of Departmentally File Servers

Any departmental fileserver must be secured to the standards above and in addition must be kept in a secure area (a dedicated machine room) which does not have general access.



Protecting confidential data

We offer guidance and support to help you protect your confidential data, whether it's files that you need to share securely or a device that requires encryption.

The PSA Academy requires that any device that holds sensitive or confidential information is encrypted. See [Encrypting your device](#) below for further advice.

If you need to share confidential data, it's vital that the files are encrypted. See [Securely sharing confidential data](#) below for further advice.

It is vital you do not transmit the encryption password via the same method as the encrypted data.

You should use another method to provide the password to the recipient. For example, if you are sending an encrypted file via email, you can send the password in a paper-based letter, or tell it to the recipient on the phone.

1.) Securely sharing confidential data

- ⇒ USB sticks
- ⇒ Encrypting zip files
- ⇒ Using Microsoft Office
- ⇒ Encrypting PDF files

USB sticks

It's much better not to put data on a USB stick at all. All members of the University now have access to Google Drive, which can be seen as a cloud based USB stick.

- ⇒ [Google Drive](#)

If it is absolutely necessary to transport data on a USB stick, make sure that all confidential data on it is encrypted.

Due to their small size, USB sticks can easily be lost or forgotten, and if not encrypted, they can then be read by anyone who finds them.

This threat is quite real, and several recent cases in the UK public sector have led to considerable media attention:

[Firm 'broke rules' over data loss](#), BBC News, 22 August 2008

[Troops' manoeuvres left in club](#), BBC News, 9 September 2008



Protecting confidential data

This threat is quite real, and several recent cases in the UK public sector have lead to considerable media attention:

[Navy to investigate security breach](#), The Guardian, 29 November 2009

[Greater Manchester Police fined over stolen data stick](#), BBC News, 16 October 2012

[East Sussex NHS Trust apologies over data breach](#), BBC News, 5 July 2015

You can buy USB sticks that include hardware based encryption. These are secure, but can usually only be used on Windows machines, on which extra software is installed.

If you wish to use one of these devices, we recommend the "Kingston Hardware Ultra Secure USB 256bit Hardware Encryption FIPS 140-2" (or another FIPS 140-2 certified USB stick). If you must use USB sticks, they are the best solution, and the only one that will satisfy some research funders.

There are a lot of other cheaper "encrypted" USB sticks out there, but only the more expensive ones properly encrypt data at the hardware level, so we strongly recommend sticking to the brands above.

Encrypting ZIP files

Another method for encrypting files is to enclose them in an encrypted zip file.

The default encryption method for ZIP files is **not secure**. It is outdated and can nowadays be broken easily. It is very important that you use the **AES-256** encryption method detailed below instead.

Windows System

On IT Services managed PCs, zip files can be created and read with the software 7-Zip. On unmanaged or personally owned PCs, 7-Zip can be install for free:

[7-Zip](#)

To create an encrypted zip file with 7-Zip:

1. Start 7-Zip, and in the main screen, select the file that you wish to encrypt
2. Click the **Add** button. This will open the **Add to Archive** window
3. Set **Archive format** to **zip**
4. Set **Encryption method** to **AES-256**
5. Enter a strong password
6. Click **OK**

You will now find a new file with a **.zip** extension in the same folder as the original file. The contents of this zip file can be accessed only with knowledge of the password.



Protecting confidential data

Encrypting ZIP files

Mac System

One option for secure zip encryption on Mac OS X is to use iZip, which is a free download:

[iZip](#)

To create an encrypted zip file with iZip:

1. Start iZip and click **New**
2. Click **Specify name**
3. In the **Save As** field, enter the name you want to give the encrypted zip file, select the location you want to save it in the **Where** field, then click **Create**
4. When asked about password protection, tick **Enable password protection** and enter a strong password
5. When asked about using encryption, choose **AES 256 bit**
6. iZip will then ask you which files and folders you want to add to the encrypted zip file. When you have finished adding your files/folders, click **Next**
7. iZip will display a summary of the options you've selected, click **Next** and your encrypted zip file will be created

Linux System

The following instructions are based on Ubuntu 14.04. Other Linux distros may be similar but not identical.

You can use **p7zip** (a Linux command line version of 7-Zip on Windows) to create encrypted zip files. You can install p7zip with the following terminal command:

```
sudo apt-get install p7zip-full
```

Once p7zip is installed, encrypted zip files can be created with the following terminal command:

```
7za a -y -tzip -p -mem=AES256 archivename.zip /path/to/filestoencrypt
```

You will be prompted to enter a password for your encrypted zip file, which will then be saved to your current location in the terminal.

You can see a list of all available commands and switches in p7zip with the following terminal command:

```
7za -h
```



Protecting confidential data

Using Microsoft Office

Windows

The latest Windows versions of Microsoft Office (2007 and later) can encrypt a file using strong encryption. Earlier versions only used very weak encryption which can easily be bypassed and should not be used.

Microsoft provide their own guidance on protecting Office files. This guidance includes instructions on encryption:

[Office 2010 and 2013](#)

[Office 2007](#)

MAC

Microsoft Office for Mac does not offer encryption for Word documents or Excel workbooks. It only offers basic password protection, which is not secure and must not be used for confidential exam material or Academy data.

However, Office for Mac can open files that have been encrypted using Office on Windows.

Encrypting PDF files

Encrypted PDF files can be a good method for transmitted data, as, once encrypted, they can be sent via email. This method has the advantage that the recipient need not store any unencrypted versions of the file on disk.

Encrypted PDF files can be read with most PDF readers, including Adobe Reader. However, for encrypting the file, special software is needed.

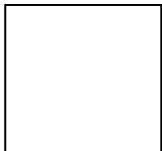
Nuance PDF Converter

PDF Converter is installed on all IT Services supported PCs, and is available to staff and students for unsupported machines and home use:

- Nuance PDF Converter

To encrypt a PDF file in Nuance PDF Converter:

1. Open the file you wish to encrypt
2. Go to **Document | Security | Secure Document**. This will open the Security panel
3. Under the **Password Security** heading, double-click on **Interactive**
4. You may see a message asking if you are sure you want to change the security settings of the document. If so, click **Yes**. The Password Security window will open
5. Select **Encrypt all document contents**
6. Tick **Allow document opening only by password** and enter a strong password in the **Document Open Password** field
7. Click **OK**. Save and close the document for the encryption to take effect



Protecting confidential data

Encrypting PDF files

Adobe Acrobat Professional

Adobe provide their own guidance on encrypting a PDF by adding a password to the file:

- [Adobe Acrobat - Securing PDFs with passwords](#)

Pdftk

Pdftk Server is a free set of command line tools for modifying PDF files. It's available for Windows, Mac and Linux:

- [Pdftk Server](#)

Once installed, you can encrypt a PDF file with the following terminal command:

```
pdftk MyFile.pdf output MyFile_encrypted.pdf user_pw PasswordGoesHere
```

Note: Replace file names and password as appropriate.

2.) Encrypting your device

Encrypting laptops and mobile devices

Device encryption is an important tool in protecting confidential data.

We offer a free service to encrypt Academy owned laptops running Windows. Please contact IT Support for more information: it_support@psa-academy.org

If you're using a device that is not owned or managed by the University, you can encrypt it yourself.

- **Windows devices**

- ⇒ We advise you to use Bitlocker to protect personal data and/or confidential information on Windows devices. If you're using a laptop or mobile device with a version of Windows that **does not** support Bitlocker, you **should not** use that device to store or process personal data or confidential information.
- ⇒ [Microsoft device encryption instructions](#)



Protecting confidential data

2.) Encrypting your device

Encrypting laptops and mobile devices

- iPhones and iPads
 - ⇒ [Set a passcode](#) to automatically encrypt your device
- Mac OS X devices
 - ⇒ [Mac OS X devices](#)
- Android devices
 - ⇒ [Android devices](#)
 - ⇒ *These instructions refer to Google Nexus devices. Other Android devices may be similar but not identical.*
- Arch Linux devices
 - ⇒ [Arch Linux devices](#)
- Fedora Linux devices
 - ⇒ [Fedora Linux devices](#)
- RedHat Linux devices
 - ⇒ [RedHat Linux devices](#)
- Ubuntu Linux devices
 - ⇒ [Ubuntu Linux devices](#)

Remember that not all devices support encryption. You must not use any unencrypted device to directly access or store confidential University information. Instead, you should use the **Virtual Desktop Service (VDS)** to access the data through a secure virtual machine.

Encryption passwords

Any encryption is only as strong as the password chosen. Short or easily guessable passwords can be broken.

Choose a strong password



Sensitive Data Handling Procedures

Academy policy requires that controls be in place to manage risk to the confidentiality, integrity and availability of sensitive data in any form and represent a minimum standard for protection of this data. Additional controls required under applicable laws, regulations, or standards governing specific forms of data (e.g., health information, credit cardholder data, student), may also apply.

Each individual who creates, uses, processes, stores, transfers, administers, and/or destroys sensitive PSA International Group™/PSA Academy™ information is responsible and accountable for complying with these standards.

Security Classifications

Categories of PSA International Group™/PSA Academy™ information based upon intended use and expected impact if disclosed. Data classifications are defined by data owners with two exceptions SSNs and credit card data that are explicitly defined and protected by policy.

Public

Information intended for public use that, when used as intended, would have little to no adverse effect on the operations, assets, or reputation of the PSA Academy™, or the Academy's obligations concerning information privacy. Information typically found on the Internet.

Internal

Information not intended for parties outside the PSA Academy™ that, if disclosed, could have adverse effect on the operations, assets, or reputation of the PSA Academy™, or the Academy's obligations concerning information privacy. Information typically found on an Intranet.

Sensitive

Information intended for limited use within the PSA Academy™ that, if disclosed, could be expected to have a serious adverse effect on the operations, assets, or reputation of the PSA Academy™, or the Academy's obligations concerning information privacy.

Creation

PSA International Group™/PSA Academy™ employees create records as part of the normal course of conducting the business of the Academy. These records document the decisions and activities of our complex educational and business enterprise. It is essential that they be created and maintained appropriately throughout their entire life cycle.

Sensitive information contained in PSA Academy™ records constitutes an area of critical concern because of the severe risk to the Academy should records be mishandled or information inappropriately accessed or disclosed. As a consequence, records containing sensitive information should exist only in areas where there is a legitimate and justifiable.

Faculties and Satellite Centres should work to identify and track all Academy records through their life cycle by way of records retention schedules (prepared in collaboration with awarding bodies, administrative offices) as defined by law. —



Sensitive Data Handling Procedures

Creation

A first priority in this effort should be the identification of sensitive information. Records schedules will document the existence of these materials, the rationale behind keeping them, and help ensure their availability during the period in which they are vital as either active administrative or historical records. Record retention schedules also will work to ensure the timely disposal of non-permanent, inactive records, thereby mitigating the risk of exposure of information when it no longer serves an active administrative or historical function.

Access

Sensitive information requires strict control, very limited access and disclosure, and may be subject to legal restrictions. In some cases, information is sensitive because it has been aggregated into a single document.

Only PSA International Group™/PSA Academy™ employees who have authorization from the data owner(s), and have a signed confidentiality agreement on file, may have access to sensitive information. Any other disclosure of sensitive information requires the written approval of the appropriate Officer of the Academy, in consultation with general counsel as necessary.

Things to remember when working with sensitive data:

- As a general rule, employees are not allowed to take sensitive data off PSA Academy™ (or to make unofficial copies)
- Where access to sensitive data has been authorized, use of such data shall be limited to the purpose required to perform Academy business.
- Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.
- Notification of a user's termination or removal of authorized access to sensitive information must be conveyed immediately to PSA Academy™ Technology.

Use, Transmission and Disposal

The following controls are **required** when using, transmitting or disposing of sensitive information.

- Do not discuss or display it in an environment where it may be viewed or overheard by unauthorized individuals.
- Do not leave keys or access badges for rooms or file cabinets containing such information in areas accessible to unauthorized personnel.



Sensitive Data Handling Procedures

Use, Transmission and Disposal

The following controls are **required** when using, transmitting or disposing of sensitive information.

- Do not discuss or display it in an environment where it may be viewed or overheard by unauthorized individuals.
- Do not leave keys or access badges for rooms or file cabinets containing such information in areas accessible to unauthorized personnel.
- When printing, photocopying or faxing it, ensure that only authorized personnel will be able to see the output.
- Store paper documents in a locked drawer *and* in a locked room, or in another secure location approved by the Data Owner.
- Properly identify such information as sensitive to all recipients, by labeling it "Sensitive," providing training to personnel, explicitly mentioning the classification, or similar means.
- Encrypt electronic information using a generally available encryption algorithm such as that built-in to common office automation applications (such as newer versions of word, excel, PowerPoint, acrobat, winzip, etc.):
 - ⇒ Placing it on removable media;
 - ⇒ Placing it on a mobile computer (e.g., laptops, PDAs, smart phones); or
 - ⇒ Sending it via e-mail to *non-wiu.edu* addresses.
- Do not send this information via email, instant message, chat or unsecured file transfer (such as FTP) unless it is encrypted.
- Follow an established and documented software development lifecycle when building applications that process sensitive information.



Sensitive Data Handling Procedures

Transport

The following controls are **required** when transporting sensitive information:

- When sending such information by mail (including U.S. Postal Service, DHL, UPS, FedEx, etc.), the sender must obtain secure, certified, tracking and signature confirmation services and use a tamper-evident sealed package. It is highly recommended that obfuscation or encryption of the sensitive data items be done before hand.
- Do not send unencrypted sensitive information by Academy mail or email.
- When carrying unencrypted sensitive information, or devices containing such information, ensure that it is physically secure at all times.
- Do not remove sensitive information from an approved secure location without prior approval of the data owner, appropriate VP area or legal counsel.
 - ⇒ As a general rule, employees are not allowed to remove sensitive data from the Academy.
 - ⇒ In the event that an individual employee or job responsibility requires sensitive information to be removed from the Academy, the information (whether electronic or paper) must be protected at all times from inappropriate disclosure. Each department/satellite center/exam centre that has individual employees or positions requiring sensitive data to be removed from the Academy must have appropriate procedures in place for protecting the data while outside the Academy and destroying the data when it is no longer required to perform the job.
- Tape media containing sensitive data should be encrypted using an approved encryption method before being sent offsite. Where feasible, alternatives to mail delivery must be utilized such as a secured, encrypted online transmission. These transmissions that utilize passwords to encrypt or decrypt data must have their own unique identifier or password.



Sensitive Data Handling Procedures

Disposal of Records, Computers and Media

- PSA Department managers are responsible for educating and training employees as to the purpose of this policy and how to dispose of information properly.
- Academy records should be destroyed in accordance with the ***Credit Card Data Retention Policy*** or departmental retention schedules.
 - ⇒ Destroy electronic instances of academy information by physical destruction or by using a DOD approved wiping method. **Reformatting a hard drive is not sufficient to securely remove all data.**
 - ⇒ Shred (crosscut shredding recommended) or pulp all highly sensitive information in paper form. This includes all transitory work products (e.g., unused copies, drafts, notes).
- Ensure that obsolete computers and electronic media (anything that can store data such as CDs, DVD, thumb drives, diskettes, iPods, etc.) are disposed of properly to ensure that no data remains. This may entail physical destruction of the computer's hard drive (or electronic media) or may instead entail electronic measures such as erasing the hard drive via a DOD approved method. Academy Technology (ATech) has procedures and technologies in place to dispose properly of old academy computers.

Note : The PSA International Company Group™'s member the PSA Security and Defence Technology Development Centre™ has a special own develop encrypted system and process for the all digital data encrypt and transport by phone, email, sms, etc format.





Credit Card Data Retention Policy

General Information

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) or by a firm specific Draft:Internal Security Assessor (ISA) that creates a Report on Compliance for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

Five different programs: Visa's Cardholder Information Security Program, MasterCard's Site Data Protection, American Express's Data Security Operating Policy, Discover's Information Security and Compliance, and the JCB's Data Security Program were started by card companies. The intentions of each were roughly similar: to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data.

The Payment Card Industry Security Standards Council (PCI SSC) was then formed and these companies aligned their individual policies to create the PCI DSS.

Retention and Disposal

Payment Card Industry (PCI) Data Security Standard (DSS) requirement 3.1 requires that the university maintain and adhere to a data retention and disposal procedures. The purpose of this procedure is to ensure that records that are no longer needed are discarded appropriately and in a timely fashion. Each area that takes credit cards as payment must periodically (annually) review these procedures to determine if any circumstances that necessitate changes in the way they retain or dispose of cardholder data.

Emory University/Emory Healthcare is required to be compliant with the PCI-DSS. Noncompliance can result in fines to merchants of at least \$10,000 per month and \$500,000 per card brand (American Express, Visa, MasterCard) if there is a data breach.

PCI DSS applies whenever account data is stored, processed, or transmitted. Account Data consists of Cardholder Data plus Sensitive Authentication Data, as follows:



Credit Card Data Retention Policy

Retention and Disposal

PCI DSS applies whenever account data is stored, processed, or transmitted. Account Data consists of Cardholder Data plus Sensitive Authentication Data, as follows:

Cardholder Data Includes:	Sensitive Authentication Data Includes:
Primary Account Number (PAN) Cardholder Name Expiration Date	Full magnetic stripe data or equivalent on a chip CAV2 / CVC2 / CVV2 / CID PINs / PIN blocks

1.1 Storage

The following credit card information is permitted to be stored only if there is an approved and documented business need. All data must be protected as described in all sections of the PCI DSS. The following card holder data, protected as required by the PCI DSS and approved by the Office of Treasury/Debt Management, is permitted to be stored under this provision:

Type of Cardholder Data

Retention Period

- Primary Account Number (PAN) Can only be stored while waiting for an authorization*
- Cardholder name Can only be stored while waiting for an authorization*
- Service Code Can only be stored while waiting for an authorization*
- Expiration Date Can only be stored while waiting for an authorization*

**** If not stored along with the PAN, this data element can be retained for up to 2 years***

The following card holder data is not permitted to be stored:

- Full Magnetic Stripe (Track 1 or 2 data) Cannot be stored
- CVV2, CVC2, CID, CAV2 Cannot be stored
- PIN / PIN Block Cannot be stored
- Pre-authorization Data including track, CVV2, and PIN information, will be retained only until completion of the authorization of a transaction.
- System and audit logs showing access to stored data must be retained for at least 1-year. Logs must be kept online and available for 90 days.



Credit Card Data Retention Policy

Retention and Disposal

1.2 Disposal

- All sensitive and credit card data must be destroyed when it is no longer required by legal, contractual, or business need.
- Techniques for disposal of data on media is as follows:
 - ⇒ **Hard disks**: must be overwritten as prescribed by the Academy Technology (ATech) Electronic Data Disposal Policy via a DOD approved method or physically destroyed.
 - ⇒ **Floppy disks**: must be shredded.
 - ⇒ **Optical media** (CD's, DVD's, Blue Ray, etc.) must be shredded
 - ⇒ **Other magnetic media**, (USB Drives, storage cards, etc.) must be overwritten by an approved method, or as prescribed by the
 - ⇒ **Paper**: must be cross-cut shredded, pulped or incinerated Academy Technology (ATech) Data Disposal Policy or otherwise destroyed.
 - ⇒ **Paper containing cardholder data**, awaiting destruction, must be stored in a secure containers secured with a lock to prevent access to its contents.
 - ⇒ Quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements must be in place.



Credit Card Data Retention Policy

DEFINITIONS

Card Verification Code or Value: Data element on a card's magnetic stripe that uses a secure cryptographic process to protect data integrity on the stripe and reveals any alteration or counterfeiting (referred to as CAV, CVC, CVV or CSC, depending on payment card)

CVC – Card Validation Code (MasterCard payment cards)

CVV – Card Verification Value (Visa and Discover payment cards)

CSC – Card Security Code (American Express)

Primary Account Number (PAN): Acronym for primary account number and also referred to as account number. Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Cardholder Data: Cardholder data is any personally identifiable information associated with a user of a credit/debit. Primary account number (PAN), name, expiry date, and card verification value 2 (CVV2) are included in this definition.

Service Code: Three-digit or four-digit value in magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such Card Holder Data Retention as defining service attributes, differentiating between international and national interchange or identifying usage restrictions.

Personally Identifiable Information: Information that can be utilized to identify an individual including but not limited to name, address, social security number, phone number, etc.

PIN: Acronym for “personal identification number.” Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder’s signature.

PIN Block: A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain subset of the PAN.



Appendix:

- ⇒ **Confidentiality Statement to all employees (2 page)**
- ⇒ **Exam Paper Register Form (1 page)**

PERSONAL INFORMATION

First Name:		Last Name:		Annexed (✓)
Title: (Mr, Mrs, Ms, Miss, Dr, Other)		Garden: (male or female)		
Date of Birth:	DD/MM/YYYY	Place:		
Nationality:		Resident:		
Passport or ID Card N°:		Driver's license N°:		
Current Address:				
National Insurance (NI) N°:		Employee's status		
Phone Number:		Email:		

I understand that depending on my future position during my work I can come in contact with confidential and sensitive data, - information about the Academy, its employees, partners, students. Examples of confidential information include, but are not limited to Academy's business documents or training materials, personal and confidential details of employees, students, business partner, - salaries, - performance evaluations, information contained in the Banner database, and charitable donations.

Therefore I agree to abide by the rules of the **Data Protection Act**, as well as other safety regulations of the PSA International Group™/PSA Academy™ as well. - especially fields of the storage, handling, delivery of the confidential data and safety of sensitive materials like exam materials.

- furthermore I understand and accept, that if I makes a false details application or if I break the PSA security regulations and the rules of data management, then it may lead to the removal of my employee status and may be subject to criminal liability. In this case I declare so then I will accept my legal responsibility, which I testify with my signature also in this present declaration.

secure line - secure - secure line - secure line - secure line - secure line - secure line *continue on the other side*



Confidentiality Statement to all employees

Additionally, upon your separation from the PSA International Group™/PSA Academy™, regardless of the reason and whether initiated by the PSA or you:

- ⇒ You must return to the PSA Academy™, retaining no copies, any and all files, records, correspondence, documents, electronic diskettes, computer compact discs, computer and electronic-mail printouts, drawings, specifications, writings and similar items, which relate to or reflect the Academy's business operations.
- ⇒ You may not use and/or disclose the Academy's confidential and/or proprietary information at any time, at any place, for any reason.

I have read and understood the all point of this Confidentiality Statement what include my responsibility as well as the regulations of the handling of confidential/sensitive datas/documents and - exam materials.

Final provisions

- A. This statement was made in two pages and three copies. One copy shall be handed to the Employee, one copy shall be for the Employer in the local office and for one other in the PSA International Co. central archives.
- B. The declarant certify and declare that the Management of PSA International Group™ /PSA Academy™ fully informed me from the relevant PSA's Policies, regulation, - procedures especially the "**Security, Integrity and Fraud Protection Policy**" main guidelines and regulations, procedures - and everything was clear and understand. - and which She/He regard as compulsory and acceptable for himself/herself, therefore she/he will be signed this statement accepting.

Declarant's Signature:	Role (Office staff/Trainer etc.)	Date: DD/MM/YYYY

Witnesses:

Name: _____

Address: _____

ID/Passport Number.: _____

Signature



Exam Paper Register.

Exam files and papers must be kept secure at all times including storage, during transport and at the location of the examination. After the examination all papers must be securely stored and returned to the Centre.

At all times, access to the exam materials must be restricted.

Centres should have written procedures to ensure the confidentiality and security of exam materials at all times. AofAQ will periodically ask for copies of this register and originals inspected by our EQAs at anytime.

Centre No: 1057

[illegible]