i-SIGMA®

CERTIFICATION SPECIFICATIONS

Reference Manual

This manual is intended for use when completing the desired i-SIGMA's NAID AAA Certification or PRISM Privacy+ Certification Application. It includes all policy, procedure and operational specifications required, including all endorsements, as well as the methods by which auditors will verify compliance. The applicability of the individual specifications listed herein is identified on the appropriate i-SIGMA's NAID AAA or PRISM Privacy+ Certification Application Form.

TABLE OF CONTENTS

SPECIFICATION APPLICABILITY

PRISM PRIVACY+ CERTIFICATION

The following specification also apply to PRISM Privacy+ Certified records management services endorsements:

All PRISM Privacy+ Certifications _____ SEC. 1, SEC. 2, SEC. 3

☐ Imaging/Digitization _____ SEC. 7

NAID AAA CERTIFICATION

The following specification also apply to NAID AAA Certified destruction service platforms and endorsements:

All NAID AAA Certifications_____SEC. 1, 4.20, 4.21, 4.24(N)

☐ Physical Media Destruction Operations
- ☐ Facility-Based _____ SEC. 2, 4.19, 4.20
  - ☐ Paper Media _____ 4.1
  - ☐ Non-Paper Media_____ 4.5
  - ☐ Micro Media_____ 4.2
  - ☐ Hard Drives _____ 4.3
  - ☐ Solid-State Device_____ 4.4
  - ☐ Product Destruction_____ 4.18
  - ☐ Operating Transfer Processing Station _____ 4.19
  - ☐ Australian PSPF: Printed/ICT: Sensitive_____SEC. 2, SEC. 5
  - ☐ Australian PSPF: Printed/ICT: Classified_____SEC. 2, SEC. 5, SEC. 6
- ☐ Mobile/Onsite_____4.20, 4.23
  - ☐ Paper Media _____ 4.1
  - ☐ Non-Paper Media _____ 4.5
  - ☐ Micro Media_____ 4.2
  - ☐ Hard Drives _____ 4.3
  - ☐ Solid-State Device_____ 4.4
  - ☐ Product Destruction_____ 4.18

☐ Overwriting or Degaussing of Electronic Media
- ☐ Facility-Based_____SEC. 2,
  - ☐ Overwriting of Hard Drives_____4.6, 4.6(QC), 4.13-4.17
  - ☐ Overwriting of Solid-State Devices_____4.4, 4.6, 4.6(QC), 4.13-4.17
  - ☐ Degaussing of Magnetic Media (Hard Drives)_____4.3, 4.7, 4.7(QC), 4.8-4.17
  - ☐ Degaussing of Magnetic Media (Mag Tape)_____4.5, 4.7, 4.7(QC), 4.8-4.17
- ☐ Mobile/Onsite _____ 4.23
  - ☐ Overwriting of Hard Drives_____4.3, 4.6, 4.6(QC), 4.13-4.17
  - ☐ Overwriting of Solid-State Devices_____4.4, 4.6, 4.6(QC), 4.13-4.17
  - ☐ Degaussing of Magnetic Media (Hard Drives)_____4.3, 4.7, 4.7(QC), 4.8-4.17
  - ☐ Degaussing of Magnetic Media (Mag Tape)_____4.5, 4.7, 4.7(QC), 4.8-4.17

i-SIGMA CERTIFICATION SPECIFICATIONS

SECTION 1: SPECIFICATIONS APPLICABLE TO ALL NAID AAA & PRISM PRIVACY+ CERTIFICATIONS

1.1 CITIZENSHIP/WORK ELIGIBILITY REQUIREMENT (Level 2)

All Access Individuals must sign a Confidentiality Agreement prior to gaining access to Confidential Data-Controller Media and employees must be legally registered to work at the Applicant location. Required files for verification include:

- Confidentiality Agreement
- Proof of Citizenship or Employment Eligibility
- U.S. Only: An I-9 for employees hired after November 7, 1986 or a proper work registration for non-citizens

AUDIT METHODOLOGY

Auditor will request evidence of the appropriate documentation in the individual files of this operation location as follows:

Where the Applicant has seven (7) or fewer Access Individuals, Auditor will request verification of applicable documentation for all Access Individuals.

Where the Applicant has more than 7 Access Individuals, Auditor will request verification of applicable documentation for a random sample, totaling 25% of the entire Access Individual List, with a minimum of 7 individuals and a maximum of 15 individuals to be selected.

1.2 INITIAL INDIVIDUAL SCREENING REQUIREMENT (Level 3 & Level 2)

Access Individuals are subject to the employment screening requirements and hiring restrictions of the following, including previous employment verification, a criminal background check, and initial employment drug-screening.

7-Year Employment History Verification *(May be completed in-house or outsourced)* **(Level 2)**

At a minimum must include the following for each place of prior employment:

- Name, City, and State of the previous employer
- Dates of employment, as reported by the employee
- Date of verification (or attempted verification if the previous employer cannot be reached)
- Indication of if the previous employer was able to verify the dates of employment.

7 Year Criminal Record Search *(Must be outsourced to a third-party background screening service following the region-specific requirements below)* **(Level 3)**

- Social Security Header Search (must be conducted prior to the criminal background investigation to ensure all counties, states, and federal district courts of residence and employment have been included and verified in the investigation)
- Federal Records Search for all Federal Districts in all states on Social Security Header Search
- Statewide records search for all states on Social Security Header Search
- County records search for all counties on Social Security Header Search

Pre-Hire or Initial Drug Screening *(Must be outsourced to a third-party background screening service)* **(Level 2)**

REGIONAL VARIANCES

- **U.S**.: County and state checks must be pulled directly from the county and state repositories. Federal checks must be pulled from the federal district courts or via PACER. The use of a secondary database is not allowed. If federal, statewide and/or county

searches are not available in a state, the applicant must complete those available and provide documentation verifying the unavailability of the other.

- **Canada**: Searches must be done on a province/territory and National basis and obtained through a third-party background search service or Canadian Police Information Centre (CPIC).
- **Outside North America**: Access Individual screening shall be reasonably consistent with what is described above to the extent permitted by law for security-related positions. Advanced description required for pre-approval.

OTHER SCREENING CONSIDERATIONS

- **Restrictive Hiring**: Where local laws and regulations allow: No person subject to a felony conviction in the last seven years for any crime involving theft (of tangible or intangible property), fraud, burglary or larceny, and no person currently incarcerated for any crime may be employed in a capacity where they may come in contact with Confidential Data-**Controller Media**. This applies to all Access Individuals.
- **Legacy Employees**: Access Individuals whose employment or relationship predates the implementation of i-SIGMA Certification policies, must be retroactively screened, and, if necessary, restricted from access to Confidential Data-Controller Media.
- **Collective Bargaining Agreements**: If a location has restrictive employee agreements in place that prevents drug screening and/or criminal record searches for certain employees, a letter must be submitted stating who and what employee screening restrictions are in place.
- **Applicability**: Where local laws and regulations allow, employment screening is applicable to all Access Individuals (other than those exempt from these requirements as mentioned above) regardless of length of service or pre-existing employment status, except where there is a restrictive employment agreement in place.

  The following Access Individuals are exempt from the Employment Verification, Drug Screening and Citizenship/Eligibility requirements:

  1) Officers, directors, owners and/or partners of the Applicant not engaged in the day-to-day operations.
  2) Others who have access to, can grant or authorize access to the Confidential Data-Controller Media to be destroyed at the applicant's location but are not engaged in the day-to-day operations; and/or
  3) Independent contractors, subcontractors, or employees thereof.
- **Owners/Stakeholders**: Any Access Individuals representing the Headquarters of the Applicant's information destruction division, minimally the President/Vice President of area &/or Audit Coordinator, whether at the location listed on this application or at another location, must have criminal background searches conducted.

AUDIT METHODOLOGY

Auditor will request evidence of the appropriate documentation in the individual files of this operation location as follows:

Where the Applicant has 7 or fewer Access Individuals, Auditor will request verification of applicable documentation for all Access Individuals.

Where the Applicant has more than 7 Access Individuals, Auditor will request verification of applicable documentation for a random sample, totaling 25% of the entire Access Individuals List, with a minimum of 7 individuals and a maximum of 15 individuals to be selected.

Auditor will verify that the results of the background check include a Social Security Header Search and a search scope of 7 years for Federal, State, and County record search of the selected Access Individuals.

1.3 ONGOING SUBSTANCE ABUSE SCREENING (Level 2)

Access Individuals are also monitored for drugs/substance abuse after the Initial Screening requirement.

The application requires the Applicant to choose between two ways of complying.

Option #1: Upon hire and thereafter on a random basis, 50% of Access Individuals are drug screened annually.

Option #2: Management has been trained in a "Substance Abuse Recognition Awareness Program" pre-approved by i-SIGMA. *(Submit i-SIGMA "Substance Abuse Recognition Training Program" (SARP) form with application for approval along with an outline of the training, or if approval has already been obtained submit the approved copy of the form for review with application.)*

AUDIT METHODOLOGY
Auditor will review the evidence of ongoing substance abuse detection/prevention based upon the method indicated.

1.4 ONGOING ACCESS INDIVIDUAL SCREENING (Level 3)

Ongoing criminal record searches are required for all Access Individuals every three years.

AUDIT METHODOLOGY
Auditor will review the evidence of ongoing criminal record search.

1.5 DRIVER QUALIFICATIONS (Level 2)

Drivers meet all licensing requirements of the governmental jurisdiction. Driving Record/License review will be conducted at minimum each quarter, or applicant will show evidence of government notification service.

AUDIT METHODOLOGY
Auditor will verify an image of commercial driver's licenses are be kept on file, updated quarterly.

1.6 WRITTEN POLICIES AND PROCEDURES AND ACCESS INDIVIDUAL AWARENESS ATTESTATION (Level 2)

The Applicant has a written policies and procedures for Individuals, conforming at minimum with applicable NAID AAA and/or PRISM Privacy+ Certification requirements, and has a written confirmation by each Access Individual stating their understanding and agreement to them. A new acknowledgement must be signed by employees on an annual basis.

AUDIT METHODOLOGY
Auditor to inspect written operational and security policies and procedures manuals and examine an appropriate random sample of employee files to ascertain and verify the employee attestation.

1.7 WRITTEN DRIVER/FIELD OPERATIONS POLICIES AND PROCEDURES (Level 2)

Applicant must have written policies and procedures addressing all field operations and security. May be included in the Applicant's general operational policies and procedures.

AUDIT METHODOLOGY
Auditor will verify that written policies and procedures exist for all field operations.

1.8 MANAGEMENT BREACH NOTIFICATION ACCOUNTABILITY (Level 2)

Applicant's Polices will include a requirement for the Applicant to report a potential release of, or unauthorized access to, that Data Controller's Confidential Data Controller Media that poses a threat to the security or confidentiality of that information immediately upon validating the existence of a data security breach incident.

AUDIT METHODOLOGY

Auditor will check procedures manual to ensure there is a written policy stating the Applicant will notify any Data Controller of a potential release of, or unauthorized access to, that Data Controller's Confidential Data Controller Media that poses a threat to the security or confidentiality of that information immediately upon validation of a data security breach incident.

1.9 ACCESS INDIVIDUAL BREACH NOTIFICATION POLICY/TRAINING (Level 2)

Prior to gaining access to confidential material, all Access Individuals must sign an acknowledgement indicating that they have received, read, and understand the Applicant's current written policies and procedures, as well as regulatory compliance issues. A new acknowledgment must be signed by Access Individuals on an annual basis.

AUDIT METHODOLOGY

Auditor will inspect Access Individual files for a signed acknowledgement of the Applicant's current written policies and procedures. This form must reference the version of the written policies and procedures that it applies to. A new acknowledgment must be signed by Access Individuals on an annual basis.

1.10 INCIDENT RESPONSE PLAN (Level 2)

The Applicant has a written Incident Response Plan for responding to suspected or known security incidents. The Incident Response Plan must include a post-incident business impact analysis and a process for documenting all incidents and their outcomes. *(see i-SIGMA Incident Reporting Log Template in i-SIGMA Certification Sample Documents)*

AUDIT METHODOLOGY

Auditor will review the Applicant's written Incident Response Plan to ensure there is a policy addressing post-incident business and Data-Controller impact analysis and documentation of all incidents and their outcomes.

1.11 UNANNOUNCED AUDIT PROCEDURES (Level 2)

The Applicant has a written policy that addresses the procedures for employees to follow during an unannounced audit. This policy must name at least one person or position of contact with physical access to the information the auditor may ask to review, which is to be contacted in the event of an unannounced audit at the destruction Facility or the office. Should circumstances prevent the designated point of contact from being available at the time of the unannounced audit, the Member Resolution Council may request additional information to be provided later.

AUDIT METHODOLOGY

Auditor will review the Applicant's written policies and procedure to verify there is an Unannounced Audit Policy, wherein is named at least one person or position to contact on-site to authorize and assist with the execution of the audit.

1.12 ACCESS INDIVIDUAL TRAINING (Level 1)

All Access Individuals must be trained annually to comply with the applicable certification requirements. The application requires the Applicant to choose between three ways of complying.

Option #1: All Access Individuals have taken and passed the i-SIGMA Access Individual Training Program (AETP). *(Submit "Access Employee Training Program Licensing" Form with application.)*

Option #2: All Access Individuals have taken and passed a third-party training course, which has been pre-approved by i-SIGMA. *(Submit i-SIGMA "Access Employee Training Program Approval" (AETP) form with application for approval along with an outline of training, or if approval has already been obtained submit the approved copy of the form for review.)*

Option #3: All Access Individuals have taken and passed an in-house training, which has been pre-approved by i-SIGMA. *(Submit i-SIGMA "Access Employee Training Program Approval" (AETP) form with application for approval along with an outline of training, or if approval has already been obtained submit the approved copy of the form for review.)*

AUDIT METHODOLOGY

Auditor will review evidence of annual training to ensure all Access Individuals have passed a training program which complies with the PRISM Privacy+ Certification requirements.

1.13 ACCESS INDIVIDUAL IDENTIFICATION ON DUTY (Level 1)

Access Individuals must always display an Applicant-issued photo I.D. badge while on duty. Badges must minimally include a photo, name, and Applicant name.

AUDIT METHODOLOGY

Auditor will inspect the Applicant policies and procedures manual to ensure there is a written policy requiring an Access Individual to always display an Applicant-issued photo I.D. badge while on duty. Auditor will also inspect Access Individuals present to verify that they are wearing photo I.D. badges.

1.14 UNIFORMED FIELD ACCESS INDIVIDUALS Level 1)

While at the Data Controller's location, drivers and other Access Individuals of contractor must always wear a specific uniform while on duty (minimum of Applicant-designated shirt) to improve recognition by Data Controllers and their agents.

AUDIT METHODOLOGY

Auditor will inspect the Applicant policies and procedures manual to ensure there is a written policy for drivers and other Access Individuals of contractor must wear a specific uniform while at the Data Controller's location. Auditor will also inspect drivers present to verify they are wearing uniforms.

1.15 RECEIPT OF MEDIA ACCEPTANCE (Level 1)

When material custody is transferred from the Data Controller's to the Service Provider's Access Individuals, the Data Controller must be provided with a receipt indicating type and quantity of materials and an acknowledgement of the services rendered.

An electronic receipt is acceptable, provided there is a verifiable electronic audit trail and the ability to provide the Data-Controller with the printed information.

If any of these services are not NAID AAA or PRISM Privacy+ Certified, but there is a NAID AAA or PRISM Privacy+ Certification that could apply, the Data Controller must be notified in writing that the Applicant does not hold those certifications. This written notification may be contained 1) on the materials receipt, 2) in the current Data Controller agreement/contract, or another written notice (including e-mail or another electronic method that may be printed) delivered by the Applicant to the Data Controller.

AUDIT METHODOLOGY

Auditor will inspect the Applicant policies and procedures to ensure that Data Controller is provided the necessary information and will inspect a copy or sample of the Data Controller documentation. Where the Applicant offers

services that are not Certifiable, the Auditor will inspect a copy or sample of the Data Controller documentation showing it declares that such services are not Certified.

APPLIES TO NAID AAA ONLY: For Facility-based operations and Transfer Processing Stations only: If a Subcontractor is used for transport prior to destruction, the Subcontractor must provide the Data Controller and the Applicant with the Data Controller receipt documentation. Auditor to verify documentation has been provided by the Subcontractor and is being utilized by inspecting a copy of a past Data Controller receipt.

1.16 VEHICLE ROADWORTHINESS (Level 1)

All vehicles used for transfer of Data-Controller Media will have the applicable government inspection for roadworthiness on file.

AUDIT METHODOLOGY
Auditor will review paperwork from the most recent inspection of all the Service Provider's commercial vehicles within the time frame stated in the applicable state law regarding the nature and frequency of these inspections. If there is a jurisdiction that does not require an inspection of commercial vehicles, Auditor will require a copy of the government statement saying so. Three vehicle records will be checked.

1.17 VEHICLE LOCKS (Level 3 *if confidential material at risk* / Level 2 *if no confidential material at risk)*

All vehicles used for transfer of Data-Controller Media will have lockable cabs and lockable, fully enclosed boxes. These vehicle cabs and boxes must be locked during transport and when unattended by Access Individuals.

AUDIT METHODOLOGY
Auditor will inspect trucks to verify that all cab doors and truck boxes are lockable and that locks work properly. Auditor will inspect the Applicant policies and procedures manual to assure that vehicle cab and box locking is addressed.

Note: If there are 3 trucks or less in either category (Mobile/Onsite Shredding and/or Collection Only), all trucks in each category must be made available for inspection. If there are 4 or more trucks in either category, 75% of the vehicles in either category must be made available for inspection. If trucks are not made available, the Applicant must provide written testimony that those trucks not presented for inspection are of equal or superior condition of roadworthiness and security. The testimony must be on Applicant letterhead and signed by an officer of the Applicant.

1.18 DATA SUBJECT RESPONSE POLICY (Level 1)

Applicant is required to have policies and procedures to respond to requests from Data Subjects. (Refer to Sample Policies and Procedures).

AUDIT METHODOLOGY
Auditor will verify appropriate Data Subject Response policies and procedures are included in the Applicant's written policies and procedures.

1.19 VERIFICATION OF ENTITY LEGAL STATUS/OWNERSHIP (Level 1)

The Applicant must demonstrate it is a legally registered entity.

AUDIT METHODOLOGY
Auditor to examine business license, Certificate of Incorporation or SEC filing.

1.20 TRANSFER OF CUSTODY (OF UNDESTROYED DATA CONTROLLER MEDIA) (Level 3)

If custody of media includes a subcontractor, the Data Controller must be notified in writing of the following information:

- Name of the organization to which custody is transferred (Subcontractor)
- The service provided by the Subcontractor

All employees of any Subcontractor accessing Data Controller media must acknowledge in writing that they understand that all media with which they come in contact is confidential, and they accept fiduciary responsibility**.**

All companies accepting custody of media must meet the Certification criteria. If Applicant does not meet the Certification criteria, then the Data Controller must be notified in writing that such service is not Certified.

The application requires the Applicant to indicate any categories of subcontractors to which custody is transferred prior to destruction Transfer of Custody.

AUDIT METHODOLOGY

Auditor will verify that the Applicant's policies and procedures include an instruction for clients to be informed when media destruction is subcontracted, providing the name of and service provided by the subcontractor, and that, where the subcontractor is non-NAID AAA Certified, the procedure requires that the client be informed of their subcontractor's non-certified status. Auditor will also verify that the Applicant's procedures related to the engagement of subcontractors requires that the subcontractor's written policies and procedures be reviewed to ensure that all subcontractors' employees are aware of their access to client information, the requirement to protect it, and the obligation to notify management in the event of a potential data security breach.

1.21 TRANSPARENCY IN BIDDING (Level 1)

Where a bid or RFQ requires or favors NAID AAA or PRISM Privacy+ Certification, the Applicant must notify the Data Controller issuing the bid or RFQ in writing of the following, when applicable:

- When the service or portion of the service being requested in the bid or RFQ is not certified at the time of the bid; and/or,
- When the service or portion of the service being requested in the bid or RFQ involves a subcontractor, and whether that subcontractor holds the required or favored certification.

(Note: Applicants should be cognizant that the results of competitive bids are often public and discovery of a misrepresentation in the bidding process could also constitute a violation of the i-SIGMA Code of Ethics, resulting in an ethics enforcement action by the i-SIGMA Complaint Resolution Council.)

AUDIT METHODOLOGY

The auditor will review the Applicant's policies and procedures to ensure that there is a written policy stating that all bids or proposals will notify potential Data Controllers if the proposed destruction service is not NAID AAA Certified and/or if subcontractors will be used for all or part of the destruction service.

1.22 SERVICE VEHICLE INSPECTION (Level 1)

Transport and/or Destruction vehicles will be inspected prior to going into service daily for of cleanliness of the collection compartment, are adequately fueled, are free from exterior damage or tire or brake or other defects that would compromise the security of transported media.

AUDIT METHODOLOGY

Auditor will check the policy and procedures manual to assure that there is a policy governing maintenance and be provided with the ongoing maintenance logs for review.

1.23 DRIVER TWO-WAY COMMUNICATIONS (Level 1)

All drivers must have a readily accessible two-way communication device.

AUDIT METHODOLOGY
Auditor to verify each driver/vehicle is equipped with a two-way communication device.

1.24 RESPONSIBLE CARE DURING CUSTODY (Level 3)

All containers, containing media, including cartons, should have operable locks to prevent loss from wind or other atmospheric conditions, and policies and procedures must state clearly that such containers, materials and media may not be left unattended or unsecure unless locked in transportation vehicle or in the secured facility.

AUDIT METHODOLOGY
The Auditor will verify that containers used in the field to transport media for destruction from the Data Controller's facility to the destruction provider's vehicle have operable locks. Auditor will inspect the Applicant policies and procedures manual to assure language requires control and security of information once transferred to Applicant custody.

Auditor to check area around collection or destruction vehicle to verify it is free from loose information-bearing media.

1.25 PERSONAL PHOTOGRAPHIC/ELECTRONIC EQUIPMENT POLICY REQUIREMENT *(Replaces 3.1)* (Level 1)

Applicant will have a written policy that identifies its method of preventing all Access Individuals' use of photographic or other electronic equipment while interacting with or in the presence of Data-Controller Media including but not limited to handheld phones.

AUDIT METHODOLOGY
Auditor will inspect a copy of policies and procedures manuals that identifies its method of preventing all Access Individuals' use of photographic and other electronic equipment while interacting with or in the presence of Data-Controller Media including but not limited to handheld phones.

1.26 VEHICLE SECURITY *(Replaces 3.2 and 4.22 (N))* (Level 2)

Transport and/or Destruction vehicles will be inspected prior to going into service daily to verify all compartments are securable and free from defects and damage that could compromise the security of media. Applicant's written policies and procedures must also define clear and effective controls to manage fleet route location detail such as GPS tracking technologies or other reporting.

AUDIT METHODOLOGY
Auditor will check policy and procedures manual to assure that there is a vehicle security control procedure in place for ensuring all media is protected within stated standards, including an inspection of tracking methodology identified in written policies and procedures.

1.27 DESIGNATION OF A DATA PROTECTION OFFICER (DPO) (Level 1)

The applicant shall designate an individual (employee or contractor) responsible for its compliance with relevant data protection and privacy regulations. This individual will be designated as the Data Protection Officer (DPO). Policies and procedures shall explicitly empower the DPO to 1) mandate compliance, including the means to achieve such compliance, and 2) define a written communications process with management to ensure compliance. A record of all DPO written communications shall be retained for a minimum of three years, unless superseded by other relevant statutory or regulatory retention requirements or limitations. In the event the DPO designation is reassigned at any point for any reason, i-SIGMA must be informed within 30 days.

AUDIT METHODOLOGY
Auditor will verify that the applicant's policies and procedures include a requirement to designate a DPO, outlining therein the duties, reporting methodologies and record keeping requirements. The auditor will also verify that the individual is an Access Employee or Contractor, and that where it is a Contractor, a valid contractor agreement is in

place, documenting the qualifications thereof. Finally, in jurisdictions requiring the DPO to register, the applicant will provide sufficient evidence to demonstrate such registration.

1.28 DESIGNATION OF AN i-SIGMA CERTIFICATION COMPLIANCE OFFICER (ICCO) (Level 1)

The applicant shall designate an employee responsible for the organization's compliance with applicable NAID AAA Certification and/or PRISM Privacy+ Certification specifications. This person will be designated the i-SIGMA Certification Compliance Officer (ICCO). Policies and procedures shall empower the ICCO to mandate compliance, as well as define a written communications process with management to ensure compliance. A record of all ICCO written communications shall be retained for a minimum of three years, unless superseded by other relevant statutory or regulatory retention requirements or limitations. In the event the ICCO designation is reassigned at any point for any reason, i-SIGMA must be informed within 30 days.

AUDIT METHODOLOGY
Auditor will verify that the applicant's policies and procedures include a requirement to designate an ICCO, outlining therein the duties, reporting methodologies, and record keeping requirements. The auditor will also verify that the individual is an Access Employee and of sufficient authority within the organization to monitor, assure, and take responsibility for compliance to relevant i-SIGMA certification requirements.

SECTION 2: SPECIFICATIONS APPLICABLE TO FACILITY-BASED NAID AAA & PRISM PRIVACY+ CERTIFICATION OPERATIONS

2.1 ACCESS CONTROL (Level 3)

Applicant must have physical, logical, and administrative controls to prevent unauthorized access to Data Controller information in the designated secure destruction area, storage area and/or staging area is effectively prevented.

AUDIT METHODOLOGY
Auditor to inspect all entrances to verify that unauthorized access to secured area is effectively prevented when media is not attended. Auditor will verify that the Applicant policies and procedures manual covers access control and unauthorized access Individuals interdiction measures.

2.2 VISITOR LOG REQUIREMENT (Level 2)

All visitors entering the secured facility must sign a log with their name, time in, affiliation, and time out, and must always be issued a "Visitor Badge" and be escorted or under the supervision of an Access Individual while in the facility. The Visitor's Log must be maintained for one year.

AUDIT METHODOLOGY
Auditor will examine visitor logs and verify the logs are maintained for one year.

2.3 SECURED AREA IN MULTI-USE FACILITIES (Level 3)

If secure information services are offered in a facility where non-related activities occur, the collection and processing of media must be in a designated (or delineated) area or secured area, with physical barriers capable of preventing and detecting unauthorized access. No unrelated services, including the processing of non-secured media may take place in designated secured areas of the facility- based destruction, except the baling of cardboard in which Data Controller media had been stored or transported.

AUDIT METHODOLOGY
Auditor to inspect building to determine that the secured area for destruction and/or media processing exists and that no baling of unshredded paper takes place in the Facility-based destruction area.

If a secured area within the building is required, it must meet the following specifications:

- There must be enough space within this area to stage all media to be destroyed.
- The wall or fence securing this area must be a minimum of six feet tall and have a lockable gate or door.
- If the wall or fence does not go all the way to the ceiling, then it must have a ceiling mounted sensor alarm inside and over the perimeter of the secure destruction, secure staging and processing areas (or similar, suitable device) to detect if and when individuals have climbed over or come through a section of the secured area fence/wall.

Where the only operations taking place within the building are related to protecting Data Controller media and information, and if all Individuals with access into the building are screened in accordance with Item 1.2 and are listed as Access Individuals, a separate secure area is not required, and the entire building is considered the secure area.

2.4 FACILITY INTRUSION & FIRE DETECTION (Level 3)

There is a third-party monitored alarm system in place and utilized to detect and alert authorities when any secure building is unoccupied for the following:

- Intrusion
- Fire (PRISM Privacy + requirement only)

AUDIT METHODOLOGY
Auditor is to inspect intrusion and fire alarm system to make sure it is operational and examine alarm test reports &/or invoices from alarm monitoring service.

2.5 CLOSED CIRCUIT IMAGE CAPTURE (Level 2)

There is a closed-circuit camera system monitoring all access points into the secure buildings/areas where confidential media is received, staged, processed and/or destroyed. All processing activities are monitored with enough clarity to identify people and their activities. There must be enough lighting during non-business hours to ensure that all images have enough clarity. Recordings must be retained for 90 consecutive days in an organized, retrievable manner.

Policies must state that i-SIGMA will be notified within 48 hours of the discovery of problems with the CCTV system which result in a loss of data.

AUDIT METHODOLOGY
Auditor to inspect the closed-circuit monitoring system to ensure that it meets criteria. This includes checking that the system has sufficient cameras and image quality to identify individuals and capture all activities in the secure destruction building from point of entry through final destruction, including any unauthorized access to the confidential information.

Auditor will also inspect the policies and procedures manual to ensure there is a written policy for notifying i-SIGMA within 48 hours of the discovery of problems with the CCTV system which result in a loss of data.

Auditor is to inspect image capture recording to verify 90-days is captures and to review four 2-minute random samples:

- Two random samples during operational hours
- One random sample during non-operational hours
- One sample from the 90th day back from the current date

Recording of operations may be suspended for playback recordings.

2.6 COLLECTION-ONLY FACILITY REQUIREMENTS (Level 2)

Collection-Only Facilities are used to store and consolidate media prior to expedited transferred to a service facility within 3 business days and must be directly linked to the secure processing facility to which the media will be ultimately stored or processed. The Collection-Only Facility must have restricted access with a monitored alarm system. The list of any and all Collection-Only Facility locations associated with

the Facility-based service operation must be included with this application.

Applicant will be required to report the number of Collection-only facilities in the application.

AUDIT METHODOLOGY
Auditor will check policy and procedures manual to assure that media for destruction is not processed and not stored for more than 3 business days and that the following are maintained:

- Access is restricted to Access Individuals
- Visitor's Log
- I.D. badges are worn by Access Individuals and visitors
- Monitored Alarm System
- In the event that the facility also stores records, recycles or bales intact/unshredded paper, or conducts other activities, the collection of media for destruction must be in a designated (or delineated) area or secured area. *(See Item 2.13)*

Auditor may or may not check the actual facility for requirements at the time of an audit.

2.7 OPERATIONAL SECURITY LOGS (Level 2)

Logs verifying the inspection and maintenance of the following Operational Security systems are checked and maintained on a monthly basis:

- Alarm System
- Lighting
- Door Locks

A Log is required verifying the CCTV system is inspected on a weekly basis, including an inspection of a minimum of five minutes of playback to ensure that all cameras and recording systems are working correctly.

Logs must be retained for one year.

AUDIT METHODOLOGY
Auditor will exam the Monthly and Weekly Operational Security Maintenance Logs and verify the are maintained for one year.

SECTION 3: ADDITIONAL SPECIFICATIONS APPLICABLE TO PRISM PRIVACY+ CERTIFICATION OPERATIONS

3.1 REPLACED BY 1.25

3.2 THIRD-PARTY NETWORK SECURITY VERIFICATION (Level 3)

Applicant is required to obtain an annual Internet Network Risk Assessment and Gap Analysis.

AUDIT METHODOLOGY
Auditor to verify a documented evidence that the Applicants online computer network has successfully achieved an acceptable security review by a competent third-party managed services provider or computer security expert.

3.3 MEDIA VAULT ACCESS CONTROL (Level 3)

Applicant must demonstrate distinct physical, administrative and logical security controls to prevent and detect unauthorized access to electronic media vaults.

AUDIT METHODOLOGY
Auditor will inspect and verify the quality of controls designed to prevent and detect unauthorized access Media Vaults, including CCTV image capture of all egress and exit, separate access control, and that all measures comply with policies and procedures used to train Access Individuals.

3.4 MEDIA VAULT ENVIRONMENTAL CONTROL MONITORING (Level 2)

Applicant must have systems in place to monitor, detect any equipment or building integrity issue that would affect the performance of necessary environmental conditions in the electronic media vault.

AUDIT METHODOLOGY
Auditor will inspect physical aspects of Media Vault environmental controls, as well as internal/external logs and invoices relevant to their monitoring and maintenance.

3.5 FINAL DISPOSITION (Level 2)

The only method for final disposition of Data-Controller media or information will be by a NAID AAA Certified service provider, holding an Endorsement appropriate to the media being destroyed, and with which the Applicant has a current contract.

The application requires the Applicant to indicate if final destruction is performed in-house or outsourced, and if the latter, to indicate the NAID AAA Certified service provider performing the destruction.

AUDIT METHODOLOGY
i- SIGMA HQ will verify NAID AAA Certified organizations listed above have a contract with the Applicant to perform all Data Controller media/information destruction.

3.6 REPLACED BY 1.26

3.7(P) PROFESSIONAL LIABILITY COVERAGE
(Must also meet 4.24(N) when applying for NAID AAA and PRISM Privacy+) **(Level 1)**

Applicant will maintain a minimum Professional Liability insurance policy of $1,000,000. (Example: Downstream Data Coverage®)

AUDIT METHODOLOGY
Auditor will examine broker confirmation (provided by Applicant) of coverage, identifying the type of coverage and indemnification limits.

SECTION 4: ADDITIONAL SPECIFICATIONS APPLICABLE TO NAID AAA CERTIFICATION MEDIA DESTRUCTION

4.1 PAPER/PRINTED MEDIA PHYSICAL DESTRUCTION ENDORSEMENT (Level 2)

Paper/Printed Media is destroyed by commercial grade destruction equipment and meets the particle size as stated by the equipment's Original Equipment Manufacturer (OEM) specifications. Acceptable deviant tolerance: 1/16 inch

The application requires the Applicant to indicate the equipment they are using to perform media destruction, which must align with the types of media endorsements they seek. (See Section 4, part 4.1 of the application for the details on the Paper Printed Destruction Equipment/Methodology).

NOTES:

- Maximum allowable particle sizes meet all regulatory compliance reasonableness requirements. Data Controllers may specify a smaller particle size at their discretion, which should be codified contractually with the Applicant.
- The Australian Protective Security Policy Framework (PSPF) Endorsement specifications

applicable to the physical destruction of paper/printed media and electronic media required verification of a separate and distinct particle size which are included in Sections 5 and 6.

- Pulping or Incineration does not apply where there is a transfer of custody to a non-NAID AAA Certified agent.

  If the Applicant owns or leases the pulping or incineration equipment and building, and as a result does not transfer custody of media to a third-party for transport or processing before media is pulped or incinerated, then the results of the pulping or incineration must effectively reduce the media to a size or condition that is unreconstructible.

AUDIT METHODOLOGY
The Auditor will verify that the particles produced by the equipment are reasonably consistent with the OEM specifications and that the equipment is of commercial grade.

Auditor will review the Screen Changing Logs during the audit.

4.2 MICRO MEDIA PHYSICAL DESTRUCTION ENDORSEMENT (Level 2)

Micro Media (Microfiche or Microfilm only) is destroyed by commercial grade destruction equipment which produces a particle size of 1/8 inch maximum dimension or less.

The application requires the Applicant to indicate the equipment they are using to perform media destruction, which must align with the types of media endorsements they seek.

AUDIT METHODOLOGY
The Auditor will verify that the particle produced by the equipment is 1/8 inch maximum or less and that the equipment is of commercial grade. Acceptable deviant tolerance: 1/16 inch.

4.3 HARD DRIVE PHYSICAL DESTRUCTION ENDORSEMENT (Level 2)

Computer Hard Drives are physically destroyed (not wiped or overwritten) in accordance with the Applicant's publicly stated and contractually agreed process which requires:

- Prior to destruction the Applicant must provide the Data Controllers with a written description of the process for destroying the hard drives.
- Serial numbers of all hard drives or DEVICEs being destroyed for each Data Controller are recorded, unless the Data Controller has signed an opt-out agreement.
- The log of recorded serial numbers is returned to the Data Controller upon the completion of the service, unless the Data Controller has opted out of this requirement.
- Hard drives must be damaged to the point where the platters will not engage.

The application requires the Applicant to indicate the equipment they are using to perform media destruction, which must align with the types of media endorsements they seek.

AUDIT METHODOLOGY
Auditor will review the Applicant's written policies and procedures for their standard physical destruction (not wiping or overwriting) of computer hard drives. Auditor will also review verification that the Data Controller has been notified of the process of destruction. Auditor will also review the serial number recordation log and any opt-out agreements Data Controllers signed.

4.4 SOLID-STATE DEVICE PHYSICAL DESTRUCTION ENDORSEMENT (Level 2)

Solid-State Devices are physically destroyed (not wiped or overwritten) in accordance with the Applicant's publicly stated and contractually agreed method of destruction which includes:

- Prior to destruction the Applicant must provide the Data Controllers with a written description of the process for destroying the solid-state devices.
- Where possible serial numbers of all solid-state devices being destroyed for each Data Controller are recorded, unless the Data Controller has signed an opt-out agreement.

- Where possible, the log of recorded serial numbers is returned to the Data Controller upon the completion of the service, unless the Data Controller has opted out of this requirement.
- Solid-State Devices must be damaged to the point where they are unable to be used.

The application requires the Applicant to indicate the equipment they are using to perform media destruction, which must align with the types of media endorsements they seek.

AUDIT METHODOLOGY
Auditor will review the Applicant's written policies and procedures for their standard physical destruction (not wiping or overwriting) of solid-state devices. Auditor will also review verification that the Data Controller has been notified of the process of destruction. Auditor will also review that where possible; the serial number recordation log and any opt-out agreements Data Controllers have signed.

4.5 OPTICAL MEDIA/MAGNETIC TAPE MEDIA ENDORSEMENT (Level 2)

Non-Paper Media primarily consisting of Optical or Magnetic Tape must be destroyed in accordance with the Applicant's publicly stated and contractually agreed method of destruction. Any method that deviates from the Applicant's publicly stated and contractually agreed method of destruction must be communicated to the Data Controller in writing.

The application requires the Applicant to indicate the equipment they are using to perform media destruction, which must align with the types of media endorsements they seek.

AUDIT METHODOLOGY
Auditor will review the Applicant's written policies and procedures for their standard physical destruction of Optical Media or Magnetic Tape Media. Auditor will also review written policies and copies of documentation provided to the Data Controller for methods of destruction that deviate from the Applicant's publicly stated and contractually agreed method.

4.6 HARD DRIVE AND/OR SOLID-STATE DEVICE OVERWRITING ENDORSEMENT (Level 2)

The Applicant has a written and verifiable process for the overwriting of Hard Drives and/or Solid-State Memory Circuits (Devices) specifying the following:

1. Process for acceptance, identification & recording of serial numbers/unique identifiers and tagging of device(s).
2. Wiping Software Product used
3. Verification Software used (must differ from #2)
4. The method of quality control in place to ensure all information has been removed from the erased media.
5. The recordkeeping audit trail for the device throughout entire overwriting process
6. Issuance of a receipt or Certificate of Destruction reflecting unique identifiers is provided to client indicating device(s) have been erased.
7. The documentation left with Client to indicate if any drives failed the wiping process. This document must include the unique identifiers of those drives, regardless of any unique identifier recordation opt-out agreement that may be in place. If any non-erased drives are left with the Client, this document must also state that custody of the device(s) is being transferred back to the Client.

The application requires the Applicant to indicate the types of Solid-State Devices they overwrite, which will be used to determine the type of Control Devices needed for the Applicant to overwrite during the audit.

(Additional components of the Overwriting Process are defined in the Overwriting Process Questionnaire.)

AUDIT METHODOLOGY
NOTE: If the applicant seeks both Hard Drive and SSD Overwriting Endorsements, both A and B below are performed separately, and a Supplemental Forensic Fee will apply.

A) **Hard Drive Overwriting**: Auditor will review Questionnaire responses and the Applicant's written policies and procedures detailing their standard Hard Drives process.

Applicant will demonstrate its ability to successfully erase Hard Drives by:

Completing overwriting on two (2) control devices provided to Applicant during the audit. These devices will have been preformatted with a known amount of control data which must be erased and returned to the auditor prior to departure. These will be sent to a data recovery service to verify that the data is not conventionally retrievable. If any devices are found to be containing data, Applicant will NOT be NAID AAA Certified.

Random selection of two (2) devices from the Applicant's processed inventory. The Auditor will randomly select the two (2) erased devices which will be sent to the data recovery service to verify that the data is not conventionally retrievable. These will be returned to Applicant after testing is completed. If any devices are found to be containing data, Applicant will NOT be NAID AAA Certified.

Auditor will observe the process for at least one drive.

B) **SSD Overwriting**: Auditor will review Questionnaire responses and the Applicant's written policies and procedures detailing their standard Solid-State Device Overwriting process.

Applicant will demonstrate its ability to successfully erase SSDs by:

Completing overwriting on two (2) control devices with consistent storage structure provided to Applicant during the audit. These devices will have been preformatted with a known amount of control data which must be erased and returned to the auditor prior to departure. These will be sent to a data recovery service to verify that the data is not conventionally retrievable. If any devices are found to be containing data, Applicant will NOT be NAID AAA Certified.

Random selection of two (2) devices from the Applicant's processed inventory. The Auditor will randomly select the two (2) devices which will be sent to the data recovery service to verify that the data is not conventionally retrievable. These will be returned to Applicant after testing is completed. If any devices are found to be containing data, Applicant will NOT be NAID AAA Certified.

Auditor will observe the overwriting process for at least one device.

4.6(qc) QUALITY CONTROL: PLANT-BASED AND/OR ONSITE HARD DRIVE/SOLID-STATE DEVICE OVERWRITING (Level 3)

The quality control software manufacturer is different than the software manufacturer, and that the Access Individual performing the quality control is different than the person that performed overwriting on the device. For Onsite Overwriting, if the same Access Individual performs both overwriting and quality control, the Auditor will determine whether the quality control procedures in place are effective.

A specific number or percentage of erased devices, as determined by the Applicant, is selected for quality control assessment on a routine basis. For Onsite Overwriting, the Quality Control assessment is performed at each Client's site, and deemed successful, prior to leaving the site.

If the quality control assessment reveals recoverable data from an erased drive, all devices processed since the last successful quality control assessment will be reprocessed. Instructions that a log must be kept of all quality control assessments to include:

- The date of the check
- The quantity of devices checked
- The outcome (fail/pass)
- A description of corrective actions taken as the result of any failed quality control checks.
- Serial numbers/Unique Identifiers of all devices that fail the overwriting process must be recorded in the Quality Control log, regardless of any unique identifier recordation opt-out agreement that may be in place.

AUDIT METHODOLOGY

Auditor will check procedures manual to assure that there is a regular quality control procedure in place for ensuring

destroyed information are within stated requirements. Auditor will also check logs to ensure the quality control checks are being performed within the timeframes established by the written policy.

4.7 MAGNETIC MEDIA DEGAUSSING ENDORSEMENT (Level 2)

The application requires the Applicant to indicate whether degaussing will be performed Facility-based, Mobile/Onsite or both.

The Applicant must have a written and verifiable process for the degaussing of Hard Drives, which includes the following:

- Procedure for acceptance, identification & recording of serial numbers and tagging of Hard Drives. *(See Item 4.14)*
- Identification of degaussing equipment is listed on the National Security Agency's Evaluated Products List – Degausser (NSA EPL-D). *(See Item 4.8)*
- Procedure for routinely verifying and calibrating degaussing equipment according to OEM specifications. *(See Item 4.7(qc))*
- Procedure for media evaluation by a trained technician to determine the type of media, whether the media is included on the list of approved media for the degaussing equipment used, and whether any data is stored on solid state components*. (Any media with solid state components used to store data must be physically destroyed, whether the media is first degaussed. See Item 4.9)*
- A process has a method of quality control in place to ensure media is physically destroyed or degaussed within the standards stated herein. *(See Item 4.7(qc))*
- Tagging/identification and separation/isolation of degaussed media after processing *(See Item 4.15)*
- The recordkeeping audit trail for the Magnetic Media throughout entire degaussing process
- Confirmation receipt or Certificate of Destruction reflecting serial numbers is provided to client indicating that the Magnetic Media has been degaussed.

(Additional components of the Degaussing Process are defined in the required Degaussing Process Questionnaire provided by i-SIGMA.)

AUDIT METHODOLOGY

Auditor will review the Degaussing Process Questionnaire responses and the Applicant's written policies and procedures detailing their standard magnetic media degaussing process.

Applicant will demonstrate its ability to successfully degauss Magnetic Media by degaussing two (2) control devices provided to Applicant at audit appointment. These devices will have been preformatted with a known amount of control data which must be degaussed and returned to the Auditor prior to departure. These will be sent to a data recovery service to verify that the data is not conventionally retrievable. The size and type of media will be determined according to the information provided in the Degaussing Process Questionnaire and must represent the OEM's specifications and the list of approved media for the degaussing equipment used. Auditor will observe the entire degaussing process.

4.7(qc) QUALITY CONTROL: MAGNETIC MEDIA DEGAUSSING (Level 3)

Degaussing and destruction processes have a method of quality control in place to ensure media is degaussed within the standards stated herein.

- A designated individual must perform quality control regarding the frequency set by the Applicant (daily, weekly, etc.)
- A log is maintained to record quality control checks to include:
  - Date of the check
  - Name/initials of individual performing the check

- Results of the check
- Description of any corrective action
- Items checked, which minimally includes the following:
  - Degaussing is performed within the equipment OEM specifications.
  - Degaussing equipment is verified for proper calibration and operation using specialized equipment designed for this purpose, and in accordance with the degaussing equipment's OEM specs. An equipment verification and calibration log is maintained to record all instances of equipment verification. *(See Item 4.12)*
  - Sample media has been sent to a data recovery service at the rate of frequency recommended by the degaussing equipment OEM specs.
  - If data was recovered by the recovery service action must be taken. *(See Item 4.11)*
  - Serial numbers/Unique Identifiers must be recorded for all media degaussed. *(See Item 4.14)*
  - Opt-out agreements are maintained for every customer for whom serial numbers/unique identifiers are not being recorded. *(See Item 4.14)*
  - The devices degaussed must match the number of devices that were brought into the facility.
  - Degaussing is completed within 30 days, unless there is a written agreement with the client stating otherwise. *(See Item 1.13)*

AUDIT METHODOLOGY

Auditor will check procedures manual to assure that there is a regular quality control procedure in place for ensuring destroyed information are within stated requirements. Auditor will also check logs to ensure the quality control checks are being performed within the timeframes established by the written policy.

4.8 USE OF NSA LISTED DEGAUSSERS (Level 2)

The equipment used by the Applicant for Degaussing (not wiping or overwriting) Magnetic Media is listed on the National Security Agency's Evaluated Products List – Degausser (NSA EPL-D), and therefore is approved for degaussing Magnetic Media (i.e. computer hard drives or tapes) with the recommended Oersted level for the specific media being degaussed by the Applicant.

Degaussing is performed for media within the range of Oersted listed on the NSA EPL-D list for the specific type of equipment used, and according to the OEM specifications for the specific media being degaussed. These specifications must be listed by media type. When degaussing a media with coercivity that is not within the degaussing equipment's approved range of Oersted, the Applicant will notify the customer in writing of the receipt of a non-NAID AAA Certified service.

The application requires the Applicant to indicate the equipment used to perform degaussing.

NOTE: Exception to this requirement available upon written request to i-SIGMA subject to a requirement to notify a Data Controller of the use of a degausser that is not NSA-Listed.

AUDIT METHODOLOGY

The Auditor will verify that the Applicant's degaussing equipment is included on the National Security Agency's Evaluated Products List – Degausser (NSA EPL-D), and that the media degaussed fall within the range of Oersted listed on the NSA EPL-D list. The auditor will also verify that the Applicant's degaussing process is in accordance with the equipment's OEM specifications for the specific media being degaussed.

The auditor will verify that the Applicant's written policies and procedures includes a requirement to notify customers in writing of the receipt of a non-NAID AAA Certified service when evaluation of media reveals that the media's coercivity is not within the degaussing equipment's approved range of Oersted.

4.9 TRAINING OF DEGAUSSING TECHNICIAN(S) (Level 1)

All technicians operating degaussing equipment and evaluating media to be degaussed have been trained on the proper use of the equipment, the types of media the equipment can effectively degauss, and how to evaluate media to determine their compatibility with the degausser. This training must be completed and documented prior to granting the technician access to the degaussing equipment or media, and then on an annual basis.

AUDIT METHODOLOGY

Auditor will review the Applicant's written policies and procedures to ensure there is a written policy for all technicians evaluating media and operating degaussing equipment to be trained on the proper use of the equipment, the types of media the equipment can effectively degauss, and how to evaluate media to determine their compatibility with the degausser, prior to being granted access to degaussing equipment or media, and then on an annual basis. Auditor will also review documentation to confirm that any Access Individuals operating degaussing equipment or evaluating media has been trained.

4.10 DESTRUCTION OF MAGNETIC MEDIA ALSO CONTAINING SOLID-STATE DEVICES (Level 2)

All media are evaluated prior to degaussing by a trained technician to determine the type of media, whether the media is included on the list of approved media for the degaussing equipment used, and whether any data is stored on solid state components. *Any media with solid state components used to store data must be physically destroyed, regardless of whether the media is first degaussed*.*

A log is maintained to track evaluated media, to include date, manufacturer, manufacturer serial number (or unique identifier), type of media, whether the media is included on the list of approved media for the degaussing equipment used, indication of any solid-state components or lack thereof, and final disposition (i.e. physical destroyed or degaussed).

**Magnetic media manufactured after 2010 may contain solid state components.*

AUDIT METHODOLOGY

Auditor will review the Applicant's written policies and procedures to ensure that there is a written policy for evaluating media prior to degaussing and that a log of all instances of media evaluation is maintained. Auditor will also verify that the Applicant has a written policy indicating that the final disposition of any media with solid state data storage components is physical destruction of the media.

4.11 THIRD-PARTY TESTING OF DEGAUSSING EFFICACY (Level 3)

Sample media are routinely tested by a third-party data recovery service at the rate of frequency recommended by the OEM specifications, and no less than once per year. Such tests must indicate that no recoverable data exists on the tested media.

The Applicant routinely submits sample media to a data recovery service to verify that no usable data can be conventionally recovered from media degaussed with the equipment listed herein, at the rate of frequency recommended by the equipment's OEM specifications and no less than once per year.

If no recommendation for testing is made by the manufacturer, ongoing testing of media is not required, other than annual testing performed by i-SIGMA.

The Applicant has a written policy for addressing reports from the data recovery service which indicate data was recovered from one or more media. This policy must minimally include the following:

- Evaluation of the recovered data to determine the nature and cause of the failure. Evaluation should include additional testing, either in-house or using a third party, if necessary, to reach a reasonable determination.
- Recalibration or reconfiguration of equipment.
- Degaussing equipment will be verified for proper calibration and operation using specialized equipment designed for this purpose, and in accordance with the degaussing equipment's OEM specifications once the issue(s) have been addressed and corrected.
- Third party testing of additional sample media once the issue(s) have been addressed and corrected.

Clients must be notified in writing of the receipt of non-certified services until the issue has been corrected and a report from the third-party lab indicates no usable, recoverable data on tested media.

AUDIT METHODOLOGY
Auditor will review written policies and procedures and equipment OEM specification to ensure there is a written policy and procedure for submission of sample media to a data recovery service, at the rate of frequency recommended by the equipment's OEM specifications and to verify that no usable data can be recovered from media degaussed with the equipment listed herein. Auditor will also verify a written policy for addressing reports from the data recovery service which indicate data was recovered. Auditor will review test reports from all tests performed by a data recovery service within the last 12 months. If any tests were returned with a report of usable data, the auditor will also review documentation verifying that the Applicant's response to such report(s) is in compliance with the requirements specified herein.

4.12 MAINTENANCE OF A DEGAUSSING EQUIPMENT CALIBRATION VERIFICATION LOG (Level 2)

A log shall be maintained to record all instances of equipment calibration verification, using specialized equipment designed for this purpose, and in accordance with the degaussing equipment's OEM specifications. Equipment that utilizes OEM built-in verification for proper calibration and operation satisfies this requirement.

AUDIT METHODOLOGY
Auditor will review the Applicant's written policies and procedures to ensure that there is a written policy for verifying degaussing equipment for proper calibration and operation and that a log recording all instances of equipment verification is maintained. The Auditor will conduct a field test with i-SIGMA-issued equipment to ensure degaussing equipment is properly calibrated and operating effectively, in accordance with OEM specifications.

4.13 DESTRUCTION TIME FRAME FOR ELECTRONIC OVERWRITING AND DEGAUSSING (Level 2)

Standard operating procedures states that the physical destruction, Hard Drive overwriting, or Magnetic Media degaussing is completed within 30 days, or the policies and procedures, the terms and conditions, and contracts used by the applicant must specify and reflect the actual time frame in which destruction is performed.

AUDIT METHODOLOGY
Auditor will check procedures manual to assure that there is a procedure stating that all media are destroyed, erased, or degaussed within requisite timeframe and verify the timeframe indicated by the applicant. Auditor will examine any unprocessed equipment in staging areas and CCTV image capture to detect unprocessed inventory exceeding the 30-day time frame. Exceptions include acts of God, breakdowns or client instruction (or permission) to retain media for a longer period.

4.14 ELECTRONIC ERASURE UNIQUE IDENTIFIER TRACKING (Level 2)

The Applicant has written and verifiable processes for the following:

- Manufacturer serial numbers or unique identifier of all media being degaussed for each client are recorded, unless the client has signed an agreement opting out of this requirement. Any opt out agreement must state that the Applicant is obligated, under NAID AAA Certification standards, to have the client sign the agreement if they choose to not have their serial numbers or unique identifier recorded.
- The log of recorded unique identifiers of degaussed media is returned to the client upon the completion of the service unless the client has opted out of this requirement.
- A log of recorded unique identifiers, a log of clients that have opted out of unique identifier recordation, copies of opt-out agreements and copies of calibration equipment verification logs are retained for a specified length of time, as documented in the Applicant's written policies, or in accordance with client agreements or contractual stipulations.
- All media is tagged, or otherwise marked, to identify and distinguish the overwritten or degaussed media from that which have not yet been erased degaussed.

AUDIT METHODOLOGY
As part of their methodology, the Applicant must record the serial numbers/unique identifiers of all media being degaussed for each client and return such list to the client, unless an opt-out agreement has been signed. Auditor will also review the Applicant's written policies and procedures for the following:

- An instruction that all unique identifiers of degaussed media are logged and returned to the client after the completion of the service unless the client opts out by signing an opt-out agreement.
- An instruction that if the client has opted out of having unique identifiers recorded, they must sign an opt-out agreement that clearly states that the recordation of unique identifiers is a NAID AAA Certification requirement.
- An instruction that a log of recorded unique identifiers, a log of clients that have opted out of unique identifier recordation, copies of opt-out agreements and copies of equipment verification and calibration logs are retained for a specified length of time, as documented in the Applicant's written policies, or in accordance with client agreements or contractual stipulations.

Auditor will also review unique identifier logs and opt out agreement logs.

4.15 POST DESTRUCTION DELINEATION OF ELECTRONIC MEDIA (Level 2)

All electronic and magnetic media is tagged, or otherwise marked or segregated in a manner that effectively identifies and distinguishes it from unprocessed media from that which has been overwritten of degaussed.

AUDIT METHODOLOGY
Auditor will review the Applicant's written policy and process of tagging, or otherwise marking the media to identify and distinguish erased or degaussed media from those that have not yet been erased or degaussed.

4.16 RESPONSIBLE DISPOSAL OF DESTROYED ELECTRONIC WASTE (Level 1)

Destroyed remnants of hard drives and circuit boards must be disposed (sold, gifted, or discarded) in a responsible manner, which includes a requirement that the recipient of the destroyed electronic media hold verified ISO 14001 certification.

*Recyclers with alternative certifications may be eligible if their certification requires ISO 14001

Applicant must attach a list of all current recipients of destroyed paper/printed media, micro media and hard drives, indicating the final disposition of materials by the recipients.

Requests for a hardship exemption must be submitted in writing to the Member Resolution Council.

AUDIT METHODOLOGY
Auditor will review list of recipients and manner by which computer hard drives are disposed. Auditor will verify that the Applicant has written agreements in place to support stated responsible disposal. Auditor to check waste receptacles and area directly outside of the information destruction building/area to see that no computer hard drives whether destroyed or intact has been deposited in waste receptacles.

4.17 ELECTRONIC RECYCLING PERMIT COMPLIANCE (Level 1)

Where local, state, and federal permits/licenses are required for the recycling of computer equipment, the Applicant will verify compliance.

AUDIT METHODOLOGY
Auditor to examine permits/license required for the recycling of computer or electronic equipment, if applicable.

4.18 PRODUCT DESTRUCTION ENDORSEMENT (Level 2)

Product Destruction is destroyed in accordance with the Applicant's publicly stated and contractually agreed method of destruction which includes:

- Product Destruction is provided in a manner consistent with the Applicant's policies and procedures manual and as publicly stated and contractually agreed.
- The policies and procedures manual must state that Data Controller receiving the product destruction endorsement will be provided a detailed account of the process used to destroy the specific product in advance of the project. Such product destruction agreements must be kept on file for 3 years from the date of the destruction.
- Access Individual Confidentiality Agreements must contain language wherein the person agrees that products accepted for destruction are to be considered confidential and that removal or use by the person is a violation punishable by dismissal and subject to possible legal prosecution.

AUDIT METHODOLOGY
Auditor will review the Applicant's written policies and procedures for their standard Product Destruction.

Auditor will also review verification that the Data Controller has been notified of the process of destruction with a detailed account of the process used to destroy the product. The notification to the Data Controller must be kept on file for 3 years from the date of destruction. Auditor will review the Access Individual confidentiality agreements to verify that language stating that the person agrees that products accepted for destruction are to be considered as confidential and that removal or use by the person is a violation punishable by dismissal and subject to possible legal prosecution. Auditor will verify policies and procedures specifically state that clients receiving product destruction services will be provided a detailed accounting of the process used to destroy the specific product in advance of the project, and that such product destruction agreements be kept on file for 3 years from the date of the destruction.

4.19 OPERATION OF TRANSFER PROCESSING STATIONS AND FACILITY-BASED (Level 3)

APPLICABLE TO: NAID AAA CERTIFICATION UTILIZING TRANSFER PROCESSING STATIONS

Transfer Processing Stations are facilities where media are temporarily collected and may be sorted or otherwise processed prior to shipment to a NAID AAA Certified Facility-based media destruction operation and is required to meet all requirements of a NAID AAA Certified Facility-based operation with except for the destruction.

- For Transfer Processing Stations, the confidential material must be transferred to a Facility-based Destruction Operation within 15 business days. If transfer does not occur in the stated timeframe, the Data Controller must be notified in writing.

APPLICABLE TO: NAID AAA CERTIFICATION for FACILITY-BASED OPERATIONS

- The destruction of confidential media must take place within 3 business days from the arrival at the destruction facility, unless Applicant has a written agreement signed by Data Controller indicating a different time frame for media destruction.
- For purges, the destruction of confidential media must take place within 15 business days. If destruction does not occur in the stated time frame, the Data Controller must be notified in writing.

AUDIT METHODOLOGY
Auditor will inspect the Facility/Transfer Processing Center to ascertain compliance with all certification requirements of the relevant Facility-based certification except those related to secure destruction not applicable to the Transfer Processing Station. The Auditor will check the policy and procedures manual, the written agreement signed by Data Controller indicating a different time frame for media destruction, the inventory of undestroyed media, and video image capture to assure that all media is destroyed within the stated timeframe. Exceptions include acts of God, breakdowns or Data Controller notification to retain media for a longer period.

4.20 QUALITY CONTROL MONITORING OF DESTRUCTION PROCESS (Level 3)

The destruction process has a defined method of quality control in place to ensure destroyed information is as required by NAID AAA Certification, and/or as publicly stated and contractually agreed.

AUDIT METHODOLOGY
Auditor will verify that policy and procedures manual include a quality control process verifying media is/are destroyed in conformance with NAID AAA Certification requirements and as publicly stated and contractually agreed. Auditor will physically inspect and or witness such processes during the audit to verify media is/are

destroyed in conformance with NAID AAA Certification requirements and as publicly stated and contractually agreed.

4.21 RESPONSIBLE DISPOSAL REQUIREMENT (Level 1)

- Destroyed paper/printed media and micro media must be disposed (sold, gifted, or discarded) in a responsible manner, which does not include any type of reuse.
- Destroyed remnants of hard drives and circuit boards must be disposed (sold, gifted, or discarded) in a responsible manner, which includes a requirement that the recipient of the destroyed electronic media hold verified ISO 14001 certification.
  *Recyclers with alternative certifications may be eligible if their certification requires ISO 14001
- Applicant must attach a list of all current recipients of destroyed paper/printed media, micro media and hard drives, indicating the final disposition of materials by the recipients.
- Refurbished electronic equipment, where all memory devices have been overwritten or otherwise erased by an NAID AAA Certified for Hard Drive and/or Solid-State Device Overwriting may be sold provided the Data Controller has been informed.
- Requests for a hardship exemption must be submitted in writing to the Member Resolution Council.

AUDIT METHODOLOGY
Auditor will review list of recipients and manner by which paper/printed media, micro media and computer hard drives are disposed. Auditor will verify that the Applicant has written agreements in place to support stated responsible disposal. Where Applicant is refurbishing electronic equipment, auditor will verify Applicant is transparent with Data Controller.

4.22(N) – Replaced by 1.26

4.23 ON PREMISES DESTRUCTION REQUIREMENT
(NAID AAA – MOBILE/ONSITE SERVICE PLATFORM ONLY) **(Level 3)**

Applicant must perform information destruction services on the Data Controller's premises.

AUDIT METHODOLOGY
Auditor will verify that the Applicant policies and procedures manual indicates that mobile destruction services must be performed at the Data Controller's site unless there is a written Data Controller agreement stating otherwise. For purposes of this requirement, an Offsite Records Center is considered the Data Controller's site when all media for destruction is generated from retained records therein.

4.24(N) GENERAL LIABILITY COVERAGE
(Must also meet 3.7(P) when applying for PRISM Privacy+) **(Level 1)**

Applicant will maintain a minimum General liability insurance (aggregate or umbrella) policy of $2,000,000.

AUDIT METHODOLOGY
Auditor to examine valid insurance documents, which could be an ACORD Certificate, a certificate of insurance or a letter from broker verifying coverage limits. Letter must be dated no earlier than one month prior to audit showing the limit to be in the amount of $2,000,000 or more.

SECTION 5: AUSTRALIAN PSPF ENDORSEMENT: PAPER/PRINTED MEDIA AND ICT MEDIA PROTECTIVELY MARKED OFFICIAL: SENSITIVE

Below are the criteria obtain NAID AAA Certification with PSPF endorsement for Paper/Printed Media and ICT Media protectively marked OFFICIAL: Sensitive. NOTE: To obtain NAID AAA Certification with PSPF

5.1 PAPER/PRINTED MEDIA AND ICT MEDIA PROTECTIVELY MARKED OFFICIAL: SENSITIVE (Level 2)

To obtain PSPF Paper/Printer Media and ICT Media protectively marked OFFICIAL: Sensitive, an Applicant must be capable of meeting the specifications stipulated in Section 5.9. OFFICIAL: Sensitive information must be same-day destruction.

AUDIT METHODOLOGY

Auditor will verify the Applicant has equipment capable of producing the OFFICIAL: Sensitive particle size for ICT Media specified in 5.9 Criteria for Media Selected.

Auditor will verify that Applicant's Policies and Procedures as well as Access Individual training must reflect that OFFICIAL: Sensitive Paper/Non-paper, or ICT media will be reduced to this particle size.

Auditor will verify that the Applicant's Policy and Procedures Manual indicates that subcontracting of collection and destruction is restricted to contractors with the NAID AAA Certification with PSPF endorsement for Paper/Printed Media and ICT Media protectively marked OFFICIAL: Sensitive

Auditor will verify that the Applicant's Policy and Procedures Manual details same-day destruction process.

5.2 CONTRACTS: SUBCONTRACTOR REQUIREMENTS (Level 2)

If Applicant subcontracts the collection, transportation and destruction of media, the subcontractor must have NAID AAA Certification with PSPF endorsement for Paper/Printed Media and ICT Media protectively marked OFFICIAL: Sensitive

AUDIT METHODOLOGY

Auditor will verify that the Applicant's Policy and Procedures Manual indicates that subcontracting of collection and destruction is restricted to contractors with the NAID AAA Certification with PSPF endorsement for Paper/Printed Media and ICT Media protectively marked OFFICIAL: Sensitive

5.3 COLLECTION AND TRANSPORTATION: WITNESSED DESTRUCTION POLICY (Level 1)

The Applicant permits agencies to escort and witness the transportation and destruction of the media.

AUDIT METHODOLOGY

Auditor will verify that the Applicant's Policy and Procedures Manual indicates that the Applicant permits the agencies to escort and witness the transportation and destruction of the media.

5.4 COLLECTION AND TRANSPORTATION: NO CONTAINER CONTENTS TRANSFER OR EVACUATION POLICY (Level 1)

The contents of secure document bins or waste bags must not be emptied into the rear of the truck and are not to be transferred or tipped into other bins at the agency's premises or in the rear of the truck.

AUDIT METHODOLOGY

Auditor will verify that the Applicant's Policy and Procedures Manual indicates that secure document bins or waste bags must not be emptied into the rear of the truck and are not to be transferred or tipped into other bins at the agency's premises or in the rear of the truck.

5.5 COLLECTION AND TRANSPORTATION: DEDICATED ROUTE POLICY (Level 2)

The Applicant must collect agency media on dedicated trips to reduce the risk of information being compromised at other collection points and decrease the timeframe between collection and destruction.

AUDIT METHODOLOGY

Auditor will verify that the Applicant's Policy and Procedures Manual indicates that the collection of media is collected on dedicated trips.

5.6 COLLECTION AND TRANSPORTATION: DOCUMENTING PROCESSING STEPS (Level 2)

The Applicant must account for media (contained in document bins) at three separate locations:

- Loading
- Unloading
- Fed into destruction equipment

AUDIT METHODOLOGY
Auditor will verify that the Applicant's Policy and Procedures Manual indicates that media is accounted for in three separate locations. Auditor will sight records to confirm accounting is taking place.

5.7 VEHICLE SECURITY: LOCKING COMPARTMENTS/CARE AND CUSTODY IN TRANSIT (Level 3)

Vehicles must be secured to prevent unauthorized access to media including:

- Driver compartments should be secured while in transit using factory locking
- Driver compartments must be secured when loading and unloading media using factory locking
- Storage compartments containing media must be secured when the vehicle is unattended
- Vehicles should not be left unattended for more than 15 minutes while containing media
- The locking mechanism for storage compartment wing doors or roller doors must be secured with a SCEC-approved SL3 rated padlock or a padlock which meets the requirements of Australian Standards (AS 4145.4: 2002)

AUDIT METHODOLOGY
Auditor to inspect the vehicles to ensure the locking elements complies. Auditor will verify that the Applicant's Policy and Procedures Manual indicates how vehicles must be secured.

5.8 FACILITY SECURITY: SECURE UNLOADING REQUIREMENT (Level 3)

The Applicant must have an enclosed area at the facility to unload media.

AUDIT METHODOLOGY
Auditor is to inspect the facility to determine that there is an enclosed area to unload media.

5.9 FACILITY SECURITY: SAME DAY DESTRUCTION REQUIREMENT (Level 3)

Media must not be stored overnight at the facility. All media must be destroyed before the close of business (or returned to the agency).

AUDIT METHODOLOGY
Auditor will verify that the Applicant's Policy and Procedures Manual indicates that media is not stored overnight. That media is destroyed as soon as possible after unloading at the facility and is destroyed before close of business (or returned to the agency).

5.10 DESTRUCTION: POST PROCESSING INSPECTION/PARTICLE SIZE REQUIREMENT (Level 2)

The Applicant must allow agencies to inspect conveyor belts, feed chutes and cutting chambers after the destruction process is completed to ensure all media has been destroyed to the particle size requirements for the media.

The Applicant must have a Quick Reference Guide for classifications corresponding with correct mesh screen size.

The Applicant must achieve the following particle sizes for ICT Media for OFFICIAL: Sensitive

The application requires the Applicant to indicate they have the capacity to destroy media to a point it will pass through a 9 mm mesh screen size.

AUDIT METHODOLOGY

Auditor will verify Applicant's Policy and Procedures Manual on how the Applicant will achieve the resultant particle sizes.

Auditor will verify Applicant's Policy and Procedures Manual on how the Applicant will achieve the resultant particle sizes.

As part of the testing process, it is essential that the residue particles are inspected to ensure:

a) Oversized particles produced by the destructor do not exceed two percent 2%.

b) Linked particles produced by the destructor do not exceed two percent 2%.

c) No linked particles exhibit more than four (4) unseparated particles.

The auditor will process each type of media separately m a laboratory test sieve with an aperture size no greater than the smallest screen size (plus 5% tolerance) the Applicant is endorsed (or is seeking) to use. For example, if the Applicant is endorsed to 3 mm, the aperture size in the sieve is 3.15 mm. The auditor will be required to process a minimum of 100g same size per each type of media.

The auditor will use the test sieve to verify that the resultant particles are consistent with the smallest screen size the Applicant is endorsed to use.

5.11 PERSONNEL SECURITY: CRIMINAL BACKGROUND SCREENING (Level 3)

Australian National Police Checks must be conducted by a National Police Checking Service organisation accredited with the Australian Criminal Intelligence Commission (ACIC) or Australian Police agencies.

AUDIT METHODOLOGY

Auditor to verify through Applicant documentation that National Police Checks have been conducted as per section 1.4.

5.12 PERSONNEL SECURITY: LEVEL 2/NATIONAL IDENTITY PROOFING GUIDELINES (Level 3)

The Applicant must check the identity of Access Individual to Level 2 of the National Identity Proofing Guidelines upon engagement.

AUDIT METHODOLOGY

Auditor to verify through Applicant documentation that Access Individuals' identity is checked to Level 2 of the National Identity Proofing Guidelines.

5.13 PERSONNEL SECURITY: ACCESS INDIVIDUAL IDENTIFICATION BADGING (Level 1)

Applicant ID should display an issue date and expiration date.

All Access Individuals must carry photographic identification (ID), which is issued and controlled by the Applicant. An ID must have all of the following displayed:

- Photograph
- Applicant logo
- Full name or an identification number of -the Access Individual
- An expiration date
- The words 'PSPF Approved'

AUDIT METHODOLOGY

Auditor to sight an Applicant ID to confirm it has all of the following necessary components:

- Photograph
- Applicant logo
- Full name or an identification number of -the Access Individual

- An expiration date
- The words 'PSPF Approved'

5.14 PERSONNEL SECURITY: NON-CITIZEN ACCESS INDIVIDUALS (Level 3)

The Applicant must conduct a visa check on Access Individuals who are not citizens or permanent residents to ensure they hold a current work visa for the duration of their employment with the Applicant.

AUDIT METHODOLOGY
Auditor to verify the Applicant records to confirm that Access Individuals who are not citizens or permanent residents hold a current work visa.

5.15 REPORTING: SECURITY INCIDENT REPORTING REQUIREMENT (Level 2)

The Applicant must immediately contact the government agency when a security incident has occurred. The Applicant must report all security incidents to T4 within five days of the incident occurring. A detailed report of the security incident must be submitted to T4 and the government agency fourteen days after the security incident is resolved.

The Applicant must establish written procedures for the following security incidents:

- Potential release of customers information
- Unauthorised access to a customer's information.
- Unauthorised reading of a customer's information.
- Unauthorised access to discrete area while destruction process is being undertaken.

AUDIT METHODOLOGY
Auditor will check procedures manual to ensure there is a written policy stating the Applicant will meet the requirements in the timeframes set.

SECTION 6: AUSTRALIAN PSPF ENDORSEMENT: HIGH SECURITY DESTRUCTION FOR PAPER/PRINTED MEDIA AND ICT MEDIA FOR SECURITY CLASSIFIED INFORMATION

The Applicant must implement Section 6 criteria in order to obtain NAID AAA Certification with PSPF endorsement for high security destruction of Paper/Printed Media and ICT Media for security classified information.

NOTE: In addition to Section 6, implementation of Section 5, "NAID AAA Certification with PSPF endorsement for Paper/Printed Media and ICT Media protectively marked OFFICIAL: Sensitive"

6.1 HIGH SECURITY ENDORSEMENT: SAME DAY DESTRUCTION REQUIREMENT (Level 3)

To obtain NAID AAA Certification with PSPF endorsement for high security destruction of Paper/Printed Media and ICT Media for security classified information, the Applicant must meet Paper/Printer Media and ICT Media protectively marked OFFICIAL: Sensitive requirements.

Security classified information must be same-day destruction.

AUDIT METHODOLOGY
Auditor will verify that the Applicant Policy and Procedures Manual details same-day destruction process.

6.2 CONTRACTS: SUBCONTRACTOR REQUIREMENTS (Level 3)

If the Applicant subcontracts the collection and transportation of media, the sub-contractor must have NAID

AAA Certification with the High security destruction for Paper/Printed Media and ICT Media for security classified information.

If the Applicant subcontracts the destruction of media, the sub-contractor must have the equivalent NAID AAA Certification and High security destruction for Paper/Printed Media and ICT Media for security classified information.

The Applicant must ensure that sub-contractor possesses the capability of destroying each type of asset and classification of Paper/Printed Media and ICT Media to the required specifications.

AUDIT METHODOLOGY
Auditor will verify that the Applicant's Policy and Procedure Manual details who the Applicant engages for subcontracting of destruction.

Auditor to ensure that the subcontracted Applicant is endorsed for the correct type of media and classification for destruction.

6.3 FACILITY SECURITY: ISOLATED/SECURE DESTRUCTION AREA (Level 2)

The Applicant must have a discrete area within the facility where approved equipment is used to destroy media.

- A discrete area with its perimeter forming part of the existing building fabric or chain link fence at least two meters high with a gate or door that can be locked from the unsecure side (that requires a key to enter) and enables egress from the secure side (for example, a turn snib).
- The discrete area must have closed circuit television (CCTV) coverage including:
    - Image resolution able to recognise (defined as 200 lines of resolution) a person in a security cage
    - Images recorded on 25 frames per second (motion activated is appropriate)
    - Accurate colour rendition
    - Lighting appropriate to support the low light level camera capability

AUDIT METHODOLOGY
Auditor to inspect facility to verify that a discrete area housing approved equipment exists.

6.4 DESTRUCTION: PARTICLE SIZE REQUIREMENT (Level 2)

The Applicant must have approved equipment to destroy media (one of the following):

- Equipment listed in the Security Equipment Catalogue and purchased prior to March 2015
- Equipment purchased after March 2015 and assessed by an independent test house such as a National Association of Testing Authorities (NATA) test house against the T4 destructor test criteria
- Equipment listed in the United States National Security Agency's (NSA) evaluated products listings (EPL)

Approved equipment must have required screen sizes as detailed below.

Screen sizes:

The Applicant must achieve the following particle sizes for High security destruction for Paper/Printed Media/ICT Media from PROTECTED to TOP SECRET:

- PROTECTED - 9 mm mesh screen size
- SECRET and TOP SECRET - 3 mm mesh screen size

AUDIT METHODOLOGY
Auditor to sight records confirming equipment was purchased prior to March 2015 and is listed as approved equipment or sights an independent test house test report stating that the equipment has been evaluated against relevant T4 destructor test criteria or review the NSA EPL to confirm the equipment is listed

6.5 DESTRUCTION: TESTING/SAMPLING PARTICLE SIZE (Level 2)

The Applicant must have approved destruction equipment assessed by i-SIGMA auditors on each audit

AUDIT METHODOLOGY
Auditor to conduct testing and produce a test report in accordance with T4 destructor test criteria.

Auditor to retain reports and sample test results until replaced by the sample taken from the most recent audit and make them available to T4 on request.

6.6 DESTRUCTION: SCREEN-SIZE CAPABILITIES/AVAILABILITY (Level 2)

The Applicant must have 3- or 9-mm mesh screen sizes available to fit the approved equipment.

Applicant must label the diameter (in mm) of the screen size on the screen mesh itself.

AUDIT METHODOLOGY
Auditor will confirm using Vernier callipers to verify mesh screen size diameter.

6.7 DESTRUCTION: EQUIPMENT TESTING PROCEDURE/REQUIREMENTS (Level 3)

The Applicant must maintain approved equipment to ensure that media is consistently destroyed to all the particle sizes the Applicant is endorsed.

The Applicant shall permit the Auditor to collect a sample of each type of media to take away for testing if required.

Prior to the audit visit, the auditor will request the Applicant to ensure that the approved equipment (cutting chamber and waste receptacle has been cleared of waste from previous production runs).

The auditor will inspect the approved equipment to ensure the correct screen size is fitted.

The auditor will request the Applicant to destroy each type of media the equipment has been approved to destroy (for example, paper/printed media/hard drives/optical/magnetic tape/flash media).

The auditor will be permitted to collect a sample of each type of media to take away for testing if required.

As part of the testing process, it is essential that the residue particles are inspected to ensure:

a) Oversized particles produced by the destructor do not exceed two percent 2%.

b) Linked particles produced by the destructor do not exceed two percent 2%

c) No linked particles exhibit more than four unseparated particles.

AUDIT METHODOLOGY
Auditor will process each type of media separately m a laboratory test sieve with an aperture size no

greater than the smallest screen size (plus 5% tolerance) the Applicant is endorsed (or is seeking) to use.
For example, if the Applicant is endorsed to 3 mm, the aperture size in the sieve is 3.15 mm. The auditor will be required to process a minimum of 100g same size per each type of media.

Auditor will use the test sieve to verify that the resultant particles are consistent with the smallest screen size the Applicant is endorsed to use.

6.8 DESTRUCTION: VISUAL INSPECTION OF SCREEN (Level 2)

The Applicant permits agencies to visually confirm the correct mesh screen size is installed prior to destruction.

AUDIT METHODOLOGY
Auditor will verify that the Applicant's Policy and Procedures Manual requires the agency to visually confirm that the correct screen size has been fitted to the equipment.

SECTION 7: ADDITIONAL SPECIFICATION RELATED TO THE PRISM PRIVACY+ IMAGING/DIGITIZATION ENDORSEMENT

The Applicant must verify compliance with Section 7 to achieve the PRISM Privacy+ Certification Imaging/Digitization Endorsement.

7.1 EQUIPMENT OPERATION/MAINTENANCE (Level 2)

Applicant's policies and procedures will specify documentation verifying quarterly internal testing and quality assurance processes for all imaging/digitization equipment.

AUDIT METHODOLOGY
Auditor will verify that the Applicant's policies and procedures include language specifying a requirement for quarterly inspection of imaging/digitization equipment. Auditor will also inspect the record of such inspection, documenting the inspector, the result of the inspection, and any remedial action determined necessary.

7.2 MANAGEMENT REVIEW OF COMPLETION/DELIVERY READINESS (Level 1)

Applicant's policies and procedures will require management sign-off of completion and delivery readiness for each project.

AUDIT METHODOLOGY
Auditor will verify that the Applicant's policies and procedures include language specifying a requirement for management sign-off on the completion and delivery readiness of each project. Auditor will also review the record of such verifications retained by the Applicant.

7.3 IMAGING/DIGITIZATION: EMPLOYEE TRAINING (Level 1)

Applicant's policies and procedures will reflect measures by which Access Individuals are trained in the proper use of scanning/digitization equipment, and how such training is recorded.

AUDIT METHODOLOGY
Auditor will verify that the Applicant's policies and procedures include language specifying the training of Access Individuals on the proper use of imaging/digitization equipment. Auditor will also inspect employment records, or other evidence, documenting the completion of such training.

7.4 WORKSTATION ACCESS CONTROL (Level 3)

Applicant's policies and procedures and physical infrastructure must effectively prevent unauthorized access to servers and local workstations to trained and approved Access Individuals.

AUDIT METHODOLOGY
Auditor will verify that the Applicant's policies and procedures include language restricting access to workstations and terminals to authorized Access Individuals. Auditor will also inspect physical, logical and administrative controls in place to effect authorized access to workstations.

7.5 IDENTITY ACCESS MANAGEMENT (Level 1)

Applicant's policies and procedures will describe its Identity Access Management (IAM) and Control methodology for all Access Individuals.

AUDIT METHODOLOGY
Auditor will verify that the Applicant's policies and procedures include language specifying the training of Access Individuals on the proper use of imaging/digitization equipment. Auditor will also inspect employment records, or other evidence, documenting the completion of such training.

7.6 DEMONSTRABLE CHAIN OF CUSTODY (Level 2)

Applicant's policies and procedures must reflect continuous care and custody from the point the applicant takes possession of client media until ultimate disposition.

AUDIT METHODOLOGY
Auditor will verify that the Applicant's policies and procedures include language defining the continuous chain of care and custody from the point it accepts media for imaging/digitization until its final secure disposition.

Auditor will examine documentation and logs related to such care and custody, as well inspect the aspects of its physical implementation.

7.7 RECORDATION OF IMAGES (Level 1)

Applicant will record scanned, imaged, or digitized information as determined and defined in the service contract.

AUDIT METHODOLOGY

Auditor will verify that the Applicant's policies and procedures include language defining their standard and unique methodologies for recording captured information, including the medium onto which captured images and information are recorded, as well as the extent to which it will be encrypted. Auditor will verify policies and procedures clearly state that all recording of scanned, imaged, and/or digitized information shall be as described within all client contracts, and the process used shall be consistent with the process therein defined. Auditor will examine sample contracts as well as the Applicant's terms and conditions to verify reference to the recordation methodology.

7.8 PROCESS ACCOUNTABILITY (Level 1)

Applicant's policies and procedures will include a process for documenting all steps in the process for every project.

AUDIT METHODOLOGY

Auditor will verify that the Applicant's policies and procedures define the processes of documenting (electronic or analog) all steps in the imaging/digitization process, including the date/time and Access Individuals involved in each contact point and procedure. Auditor will review such documentation related to tracking of the points of contact and processing to verify such accountability is tracked and available.

7.9 ENCRYPTION OF STORED/RETAINED IMAGES (Level 2)

Applicant's policies and procedures will require all scanned, imaged, or digitized information/media will be encrypted when stored while in their care and custody.

AUDIT METHODOLOGY

Auditor will verify that the Applicant's policies and procedures include a requirement to encrypt captured information, including specifications related to such encryption. Auditor will examine evidence that such encryption is being used, the nature of such evidence to be appropriate and to the Auditor's satisfaction.

7.10 PROHIBITION ON DISSEMINATION (Level 2)

Applicant's policies and procedures, and functional operations will effectively prevent the unauthorized printing, viewing, reproduction, transmission, or distribution of client media.

AUDIT METHODOLOGY

Auditor will verify that the Applicant's policies and procedures include language forbidding unauthorized reproduction or distribution, and further verify that all Access Individuals have executed an agreement stating their understanding of the policy and potential legal and other disciplinary consequences of any violation.

7.11 EFFECTIVE, REDUNDANT IMAGE CAPTURE (Level 2)

Applicant's policies and procedures will stipulate the process of backing-up all captured/processed images, verify efficacy of redundancy at least once per day, and is to include a procedural requirement to recapture or re-record any images or information should it be discovered the back-up procedure for any batch failed.

AUDIT METHODOLOGY

Auditor will verify that the Applicant's policies and procedures require and define the process by which captured/processed images and information are redundantly backed-up, the requirement and process by which the efficacy of such redundant backed up information is verified daily, and a procedural requirement to re-capture any images or information recorded since the most recent successful verification.

7.12 IMAGE TRANSFER (Level 2)

Applicant's policies and procedures will require images and/or information be stored and transferred to the client (or agent of the client) in the format contractually agreed. Where the format is not contractually prescribed, said images and information will be encrypted to a 256-bit AES standard.

AUDIT METHODOLOGY

Auditor will verify that the Applicant's policies and procedures specify that all captured images and information be transferred to the client or agent of the client is encrypted to a 256-bit AES standard, unless contractually required to do otherwise.

7.13 DOCUMENTING FINAL DISPOSITION (Level 1)

Where the client has specified destruction of scanned/imaged media, applicant's policies and procedures will require a log for all such media destroyed, including details related to authorization, date, location of destruction, methodology, and a certificate of destruction from any service provider when outsourced.

AUDIT METHODOLOGY

Auditor will verify that the Applicant's policies and procedures specify a requirement to log all media disposition, whether disposition is accomplished by returning the media to the client, or by secure destruction on behalf of the client. Auditor will also inspect the disposition log to verify its existence, as well as verify that it documents the information designated in the specification.

7.14 FINAL DISPOSITION OPTIONS (Level 1)

Applicant's policies and procedures will require that disposition instructions for each client/project as one of the following acceptable options: 1) return to data controller (client), 2) secure storage by PRISM Privacy+ Certified organization, or 3) destruction by a NAID AAA Certified service provider. This requirement applies to all related media and information, including original, redundant, ancillary, incomplete, and/or defective media and information.

AUDIT METHODOLOGY

Auditor will verify that the Applicant's policies and procedures will specify that disposition of all media be 1) return to data controller (client), 2) secure storage by PRISM Privacy+ Certified organization, or 3) destroyed by a NAID AAA Certified service provider. Auditor will verify that where information is stored or destroyed via a contractor, their service provider is named, holds the required certifications, and that there is a contract in place specifying with the contractor the requirement to maintain said certification.

TERMS & CONDITIONS OF i-SIGMA CERTIFICATION PROGRAM PARTICIPATION

1. NAID AAA and PRISM Privacy+ Certification are optional and not required for i-SIGMA membership.
2. The Applicant must be a member of i-SIGMA in good standing and with no outstanding debt to the association to achieve and maintain Certification.
3. Owners or Senior management of the Division of the Applicant have read and understands the appropriate Certification Audit Methodology, which makes clear the documentation, facilities, and equipment that each location will be required to have available and immediately accessible to the Auditor.
4. The Applicant understands that biennially scheduled Audits are required as are part of the Certification Program. Any failure to cooperate with the scheduling of a renewal audit or failure to make accessible for inspection all documentation, facilities, and equipment on the agreed upon date, time and location identified on the *Auditor Assignment & Confidentiality Agreement* (Appointment) form may result in a course of remedial action. Applicant understands that failing to cooperate with the scheduling of a renewal audit after the six-month time frame allowance may result in a $1,000 fine (due within 30 days of notification) and a *temporary suspension* of certification until a successful completion of a compliant audit done within 90 days of notification. Additionally, applicant understands that cancelling a scheduled audit after auditor travel expenses have incurred may result in a $1,500 fine plus reimbursement of auditor travel expenses (due within 30 days of notification) and a *temporary suspension* of certification until a successful completion of a compliant audit done within 90 days of notification, and refusal of a scheduled initial or renewal audit on the day of scheduled audit may result in a $2,500 plus reimbursement of auditor travel expenses (due within 30 days of notification) and a *temporary suspension* of certification until a successful completion of a compliant audit done within 90 days of notification.
5. Application fees are non-refundable, except in the instance where the Auditor fails to conduct the audit on the date, time and location indicated on the *Auditor Assignment & Confidentiality Agreement* (Appointment) form; and when, in such circumstance, the Applicant decides to withdraw their application.
6. At no time will the label “NAID AAA Certification,” “NAID AAA Certified, “PRISM Privacy+ Certified,” or PRISM Privacy+ Certification” be applied, referenced or inferred to facilities or operations of the Applicant where 1) the location and operating details related to the facility or operation have not been specifically and formally provided to i-SIGMA for participation in the applicable Certification program, or two) the facility or operation does not have any involvement related to the collection, transport, processing, overwriting, degaussing, and/or destruction of media.
7. The Applicant must reapply for Certification on an annual basis and prior to the expiration of the current Certification. If the Applicant chooses not to reapply and/or not to submit to the required audit, it will result in loss of Certification. Loss of Certification will not affect i-SIGMA membership.
8. The Applicant understands that Certification status is public information. Information regarding renewals, lapses, certified operations and endorsements, Applicant contact information, and the Certification expiration date are displayed on the i-SIGMA website and made available to email subscribers.
9. The Applicant will hold i-SIGMA harmless from any claim of damage or loss as a result of the Applicant’s failure to achieve Certification.
10. The Applicant understands and agrees that at least 90-days of CCTV recordings must be maintained, and the Applicant must be able to produce evidence of image capture at time of an audit. If the Applicant is unable to produce the 90-days of recordings at an audit, the Applicant may be subject to a re-audit. including associated costs.
11. The Applicant understands that the specifications and fees for Certification are subject to change at the discretion of the i-SIGMA Board of Directors.
12. All of the Applicant’s employees are legally registered to work in the country to which this Application applies, and the Applicant has all necessary documentation to confirm this fact.
13. The Applicant understands that it is responsible for ensuring that background checks of current and prospective employees and any use of consumer reports for employment purposes comply with the mandates of the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.

14. If restrictive employment agreements are in place that would prevent the Applicant from conducting drug screening and/or criminal record searches, the Applicant will provide a detailed description of such restrictions with this application.
15. The Applicant understands that random Unannounced Audits are part of the Certification Program. Only if asked and not a hardship, the Applicant will allow access to an i-SIGMA Certification Auditor for purposes of conducting such Unannounced Audits. Any refusal of an unannounced audit or failure to make accessible for inspection all documentation, facilities and equipment at the time of the unannounced audit may result in requiring the Member to pay an initial fine in the amount equal to their certification application fee, payable within 30 days; an additional unannounced re-audit to take place within three (3) months; and an additional scheduled follow-up audit to occur within six (6) months (outside the Member's normal application and scheduled audit process), along with an additional fine in the amount equal to their certification application fee, payable within 90 days.
16. The Applicant understands that the i-SIGMA Member Resolution Council (MRC) may track verified egregious reports of certification non-compliance per Applicant/location and may issue fines and/or sanctions or recommend removal of certification in accordance with MRC Guidelines. Initial (new) Certified Applicants found in non-compliance will be remediated without penalty; however, any non-compliance issues will be documented to the Member record for renewal tracking. Certification Applicants renewing their annual Certification will be assisted in remediation of any non-compliant items. Any Member unable to meet compliance will no longer be eligible to retain their Certification, and a case will be opened and escalated to the MRC who will draft a recommendation and forward it to the i-SIGMA Board of Directors for a final decision. All specifications in the i-SIGMA Certification Specification Manual indicate the appropriate level of non-compliance (1, 2 or 3). Three (3) or more Level 1 non-compliant items found in an audit will be assessed a $1,000 total fine, and two (2) or more Level 2 non-compliant items found in an audit will be assessed a $1,000 total fine. Any seeming non-compliant items wherein documents (excluding policies and procedures) were not located at the time of audit may be remediated within five (5) business days with i-SIGMA staff, by providing said paperwork, without being considered in non-compliance. A first instance of a specific Level 3 specification found non-compliant during an audit is a $1,000 fine; a second instance of the same Level 3 specification found non-compliant within the following two audits will require a re-audit within 90 days along with an assessed recertification fee. A third instance of the same Level 3 specification found non-compliant within the following two audits will be escalated to the MRC for recommendation. Any multiple instances (two or more) of Level 3 non-compliance within the same audit will require a scheduled re-audit within 90 days along with an assessed recertification fee. All assessed fines must be paid within 30 days, unless the applicant chooses to appeal the findings of the audit report (meaning applicant believes there is an error in the report) or the calculation of fines, in which case a formal appeal must be submitted to i-SIGMA Headquarters no later than 30 days after the date of notification of the fine/sanction. The applicant understands that the i-SIGMA Member Resolution Council (MRC) will review appeals of i-SIGMA staff-imposed fines/sanctions, and the Applicant will be granted the opportunity to provide spoken testimony within 30 days of the formal submission of the appeal. The applicant understands that the i-SIGMA Board of Directors will review appeals of MRC-imposed fines/sanctions, and the Applicant will be granted the opportunity to provide spoken testimony within 30 days of the formal submission of the appeal. The Applicant will accept the ruling of the i-SIGMA Board of Directors as final and seek no further remedy, legal or otherwise.
17. The Applicant understands and agrees that the i-SIGMA Certification Auditor may inspect and test its access control systems related to the facilities, containers and vehicles used to provide secure destruction services during announced and unannounced audits and will not consider such inspection and testing to be a violation of the law, provided such inspection and testing does not result in property damage or the risk of personal injury and is undertaken solely for the purpose of ascertaining compliance with Certification.
18. At any time during the application and/or audit process or after Certification is achieved, the Applicant acknowledges that i-SIGMA, its agents and/or the i-SIGMA Certification Auditor may investigate or require additional information or documentation from the Applicant in order to verify information on this Application or the Certification criteria.
19. The Applicant understands and agrees that all of its employees and agents will refrain from any false or misleading claims, suggestions or references regarding Certification, including but not limited to such claims used in advertising produced in advance and/or in anticipation of Certification at some future date.
20. The Applicant understands and agrees that any change of address, ownership, or the operations/services it offers to Clients any time during a pending Certification application or audit, or while the Applicant is Certified, it must notify i-SIGMA in writing within 15-business-days of this status change. Failure to do so may result in fines, sanctions and/or revocation of Certification.
21. The Applicant understands and agrees that should it undergo a change in controlling interest in ownership, it

will notify the controlling interest that written verification must be provided to i-SIGMA within 30-calendar-days of the date the acquisition is final. The written notice must also state that the controlling interest will continue to operate within Certification standards under the new ownership and agreeing to be subject to a Certification audit within six months from the date the acquisition or change of ownership is final. Failure to apply for, or to successfully pass, an audit under the new ownership may result in removal of certification. If a member of the Multi-location certification program acquires a location that is currently NAID AAA-Certified, the i-SIGMA staff will determine if the acquired location is eligible to be added to the multi-location audit rotation cycle. The determination will be based on the member's and acquired location's compliance history. Furthermore, it is i-SIGMA policy that all locations must be audited no less than once every 3 years. Therefore, the timing of the acquired location's next audit will depend on the length of time since that location was last audited.

22. If the Applicant is certified for Facility-based operations, the Applicant understands and agrees that should it relocate to a new location it will provide written verification to i-SIGMA within 15-days of the date of the move and that it must continue to operate within Certification standards at the new location, and that it will submit to an audit within six months of the date of the move. Failure to apply for, or to successfully pass an audit at the new location, may result in removal of certification.
23. The Applicant agrees that if any location for which it is seeking Certification becomes Certified, and subsequently elects to discontinue any or all Certified operations or endorsements for such location, the Applicant must notify i-SIGMA in writing within 30-days of this status change and has an ethical responsibility to inform clients (aware of the Applicant's Certification status) of the change.
24. The Applicant understands that ALL Certifiable services/operations being promoted to the Applicant's Clients must be Certified in order to gain and maintain Certified status. If the Applicant adds a Certifiable operation after Certification has been approved, it has 6-months in which to apply for Certification of the new service/ operation. Failure to apply for and/or successfully pass an audit of all certifiable operations may result in the removal of all Certifications.
25. The Applicant understands that the i-SIGMA Auditor does NOT approve or deny Certification, and that the Auditor's findings will be submitted to i-SIGMA Certification Staff for review and processing.
26. An Applicant may be assessed an additional administrative fee due to the submission of an incomplete Certification renewal application, delaying an i-SIGMA Auditor during an audit due to unpreparedness, or requiring i-SIGMA staff involvement in post-audit remediate of non-compliance issues.

GLOSSARY OF TERMS

The following are definitions of words or terms used regarding i-SIGMA Certification Programs.

ACCESS INDIVIDUALS – Individuals who, in their capacity as an agent of the Applicant, have access to, or the capacity to grant or authorize access to the Confidential Customer Media, including but not limited to 1) employees, 2) agents of "sub-contractors" as defined herein, and/or 3) others providing any type of services to the Applicant that necessitates access to any area in which Confidential Customer Media is accessible. NOTE: Access Individuals do not include "Visitors," as defined herein, who must be under the direct supervision of an Access Individual while in the presence of Confidential Customer Media.

AETP (originally known as the Access Employee Training Program) – A computer-based employee training module that provides one option for comply with the Certification employee training requirements. The AETP is intended to familiarize Access Individuals of i-SIGMA Members with their responsibilities under i-SIGMA Certifications, as well as data protection and privacy regulations.

BRANCH/LOCATION – Any facility or place operated by an Applicant where 1) Confidential Customer Media is destroyed; or 2) stand-alone support is provided for Mobile/Onsite Operations.

BIN TIP –The process of servicing a collection bin or exchanging bins containing Confidential Customer Media to be destroyed.

COLLECTION FACILITY – A facility separate from a secure destruction facility where Confidential Customer Media is stored exactly as accepted from a customer, with no further modification of packaging and no access or processing by staff after collection. Confidential Customer Media for destruction may not be stored for a period longer than 3 business days before being transferred to a secure destruction facility.

If Confidential Customer Media is stored in a facility longer than three business days, the facility is classified as a Transfer Processing Station *(see definition and application criteria for details).*

In the event that the Applicant location maintains its own commercial records storage center, and stores/stages Confidential Customer Media generated for destruction from that facility exclusively, the facility is NOT considered a Collection Facility. However, if a records storage center is also used to store Confidential Customer Media on an intermediary basis while in transit from customer location to a separate destruction facility, it is then classified as a Collection Facility.

A Collection Facility must meet all Operational Security requirements (*see section 2 in the criteria*) as a destruction facility with the exception of a CCTV monitoring and recording system.

COMPUTER HARD DRIVES (or Hard Drives) – The memory storage device consisting of a rotating metal platter using magnetic charge to store digital code. Excludes microchips, microprocessors or storage devices typically found in PDAs, cell phones, or USB storage devices.

CONFIDENTIALITY AGREEMENT – An Agreement in which all Access Individuals acknowledge they will keep any customer media and information secure and confidential. A Confidentiality Agreement having concepts substantially similar to the sample document available to all i-SIGMA members must be signed by all Access Individuals and Non-Access Employees, and the Agreement must be kept on file by the Applicant.

Where it is not practical to have such an Agreement directly with an individual, a letter from the Subcontractor, verifying that such an Agreement has been executed by any of their agents intended to serve in the same capacity as an Access Individual would be acceptable.

CONFIDENTIAL CUSTOMER MEDIA – Documents, papers, records, or other media received by the Applicant from customers for destruction.

DATA CONTROLLER – An organization that collects Data Subjects' Personal Information in order to provide some service, e.g., banks, hospitals, insurance companies, employers.

DATA PROCESSOR – A service provider or other organization with which a Data Controller shares or allows access to Data Subjects' Personal Information in order to perform some subset of services for the Data Controller, e.g., data destruction, IT asset management, records storage, data backup, managed service provider.

DATA SUBJECT – An individual who is the subject of personal information about themselves.

DEGAUSSING – Use of a strong magnetic field to erase information recorded on Magnetic Media, such as conventional hard drives.

EMPLOYMENT HISTORY VERIFICATION – A verification of all prior employment held by an Access Individual of the Applicant over the past 7 years; the verification may be conducted internally or outsourced, at the discretion of the Applicant.

FACILITY-BASED OPERATION – Secure destruction activities—including the staging, destruction, baling, and storage of destroyed materials—housed within a secure building environment and executed using fixed-location commercial-grade destruction equipment.

LEVEL 1, 2, 3 – Refers to the offense level of non-compliance found during the audit and remediated appropriately. This correlates to the fine structure, which can be found by logging into the Members Portal and visiting "My Digital Library." Enter "Certified Documents" from there, where you will find "i- SIGMA Non-Compliance Tracking Policies and Procedures."

MAGNETIC MEDIA – Storage devices that use patterns of magnetization to imprint data on plastic or metal that has been coated with iron oxide. Examples include, but are not limited to, magnetic tapes and floppy disks.

MEDIA – Any information-bearing medium, including but not limited to paper, microfilm, microfiche, X- rays, ID badges, credit/debit cards, computer hard drives, magnetic or digital tapes, disks or cartridges.

MEDIA VAULT – A segregated, secure room or area possessing special environmental controls need to store film and tape media.

MICRO MEDIA **-** Microfiche and Microfilm

MOBILE/ONSITE OPERATION – Secure destruction activities carried out using mobile commercial- grade destruction equipment that destroys Confidential Customer Media within an enclosed and securable vehicle (truck or trailer) at the customer's site.

NON-ACCESS EMPLOYEES – Employees of the Applicant who a) are restricted from access to secure destruction areas and other areas where Confidential Customer Media is accessible; or b) have not been through, or cannot be fully vetted for, the Certification employee screening requirements. These employees must be accompanied, supervised, or escorted by an Access Employee at all times when in presence of Confidential Customer Media to be destroyed. See also: Visitors.

NON-CITIZEN ACCESS INDIVIDUAL – Employees and other agents of the Applicant who are not citizens of the country in which the Applicant location is operated.

OPTICAL MEDIA / MAGNETIC TAPE MEDIA– Optical Media (Digital Video Disks, Compact Disks). Floppy Disks. X-Rays.

OPTICAL MEDIA – Digital electronic storage devices that use laser technology to write and read data. Examples include, but are not limited to, CDs, DVDs, CD-ROMs and DVD-ROMs.

OVERWRITING – The commonly used term to describe the process of recording meaningless information on magnetic or solid-state media as method of eliminating meaningful information.

PAPER OR PRINTED MEDIA – Information printed on paper or other material that can be read by the naked eye without the assistance of a special device, such as documents, ID badges, credit/debit cards and photos.

PRODUCT DESTRUCTION - The destruction of non-information bearing items, including but not limited to contraband, product overruns, returned items (defective or useable), counterfeit items, clothing, publications, or anything which the product owner deems harmful if not definitively destroyed in a controlled and secure manner.

PURGE – An information destruction project that is defined by the Applicant and/or client as an inordinately large amount of Confidential Customer Media to be destroyed.

SOLID-STATE DEVICES (SSDs) – Data storage device where information is recorded via an electric charge. Such as Flash Media: SIMS cards, USB storage devices, PDAs and cell phones, tablets, etc.

SERVICE VEHICLE – Any vehicle operating on public streets that provides collection, delivery or processing of Customer Confidential Media.

SUBCONTRACTOR **-** Any entity the Applicant uses to provide services that are an integral part of the Applicant's destruction service and whose employees or agents have access to Confidential Customer

Media to be destroyed. Examples include providers of temporary staffing, transportation, etc. *Use of another destruction Applicant for remote locations, projects, or other special circumstances must be represented to the Applicant's clients as NOT Certified, unless such Applicant is currently Certified for the work being performed. These service providers do not need to be submitted as Subcontractors.*

TEMPORARY SUSPENSION – A company that has their certification suspended will show a designation to the effect of "Temporarily Suspended" next to their Certification on the i-SIGMA Website for the designated period of time and their Compliance Monitoring will send out a notification to that end. That company may continue to operate as a certified member until they are either brought back into good standing or their certification is terminated; in either case, the certification compliance monitoring would send an update of the new status.

TRANSFER PROCESSING STATION (or TPS) – A facility without destruction capability, and where Confidential Customer Media destined for a destruction facility is batched, sorted, cleaned or repackaged within the facility; or a facility where Confidential Customer Media is stored for more than three business days while in route to a destruction facility.

A Transfer Processing Station must meet all the same Operational Security requirements as a destruction facility *(see Application)*.

VISITORS – Any person who may enter the secure destruction area/facility (with or without Confidential Customer Media for destruction) and who is: a) not employed by the Applicant; b) working as (or for) an independent contractor for the Applicant; c) otherwise providing services to the Applicant for compensation; and/or 4) an employee from another division or Applicant location who has not met all of the Certification Employee Screening requirements and is not wearing a Photo ID badge; is considered a Visitor. All Visitors must sign an Applicant-maintained Visitor log, receive a Visitor badge, and remain under the supervision of an Access Individual at all times while in the secure destruction building, or area with Confidential Customer Media for destruction. This includes, but is not limited to, current or prospective clients, service providers such as vending machine distributors, mechanics, or technicians; employees as noted above.