**Internal Authorization # \_\_\_\_\_\_\_\_\_\_\_**

I hereby certify that the **original physical or electronic documents and data** containing \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ data provided to me by the **Requesting Organization** have been duly and securely destroyed such that reconstruction is not reasonably foreseeable.

In addition to the destruction of the original documents containing \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, I hereby certify that **all copies** of the data obtained from the **Requesting Organization**, reproduced, located, stored or found on servers, hard drives, CDs/DVDs, USB keys, laptops, paper and any other format, device or media regardless of location, have also been duly and securely destroyed such that reconstruction is not reasonably foreseeable.

The description of destruction methodologies employed contained in **Schedule A** form a part of this **Certificate of Destruction**

Recipients of **Requesting Organization** data and ultimately the institution or organization are asked to provide **Requesting Organization** with a certificate of destruction, which certifies the completion of the secure destruction activity and sets out the date, time, location and method of secure destruction employed. Where the destruction of data has been executed by an external third party, that party’s Certificate of Destruction is **appended hereto and forms a part of this Certificate of Destruction**.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| **Name**  |  | **Title** |
|  |  | *Information or Chief Technology Officer* *or equivalent senior position* |
|  |  |  |
|  |  |  |
|  |  |  |
| **Signature** |  | **Date** |

Documentation must be comprehensive of all formats, devices, and media used to access or retain Requesting Organization physical or electronic documents and data.

A response must be provided for each of Sections A to D below.

|  |
| --- |
| **A. Paper Format Destruction of Requesting Organization Confidential Information****Select one of:** |
| **** Not applicable - No storage in Paper format |
| **** The following external service provider was contracted to complete secure destruction:

|  |
| --- |
|   |

Provide the name of the service provider in the space above and **append a copy of the certificate**.Provide the **title and date of the contract** between the Requesting Organization and the service provider.Note that the certificate must set out the date, time, location and method of secure destruction employed as well as the full name and signature of the operator completing the work. |
| **** Physical destruction by staff using the following method:

|  |  |  |  |
| --- | --- | --- | --- |
| **** Incinerating |  |  |  |
| **** Shredding (cross-cut) |  |  |  |

|  |  |
| --- | --- |
| Location (Full Address): |  |
| Date (Month Day, Year): |  | Time (Hr:Min AM/PM): |  |
| Types of paper documents: |  |
| Title/Position of Staff Completing Activity: |  |
| Signature of Staff Completing Activity: |  |

 |

|  |
| --- |
| **B. Portable Media: Destruction of Requesting Organization Confidential Information (For example, CD/DVD, USB Keys/Flash Drives)****Select one of:** |
| **** Not applicable - No storage on CD/DVD or Similar Portable Optical/Magnetic Disk |
| **** The following external service provider was contracted to complete secure destruction:

|  |
| --- |
|   |

Provide the name of the service provider in the space above and **append a copy of the certificate**.Provide the **title and date of the contract** between the Requesting Organization and the service provider.Note that the certificate must set out the date, time, location and method of secure destruction employed as well as the full name and signature of the operator completing the work. |
| **** Physical destruction and/or use of data destruction software by staff using the following method(s):*NOTE: Industry best practices for the secure destruction of data are constantly evolving and this is particularly true for data in electronic format. For general information with respect to secure destruction methods, please review the NIST Guidelines for Media Sanitization at* [*http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf*](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf)*. Sanitization techniques are outlined in Section 5.*

|  |  |  |  |
| --- | --- | --- | --- |
|  Degaussing |  |  |  |
|  Grinding (platters only) |  |  |  |
|  Incinerating |  |  |  |
|  Shredding |  |  |  |
|  Sanitizing Overwrites | Number of overwrites: \_\_\_\_ | Software used (including version): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  Selective Wipes | Number of wipes: \_\_\_\_ | Software used (including version): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **** | Briefly describe the selective wiping method, method of marking or tagging of Confidential Information that makes restoration impossible­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Please confirm the device(s) selectively wiped remain under the secure custody and control of our organization, and subject to the privacy and security policies of our organization. |
|   | Please confirm the device(s) selectively wiped is/are subject to an end-of-life policy that requires secure physical destruction, degaussing (where appropriate) or complete sanitizing overwrite of the entire device/media in accordance with industry best practices, prior to the media leaving our organization’s custody and control. |
| Location (Full Address): |  |
| Date (Month Day, Year): |  | Time (Hr:Min AM/PM): |  |
| Types of electronic data: |  |
| Full Name of Staff Completing Activity: |  |
| Title/Position of Staff Completing Activity: |  |
| Signature of Staff Completing Activity: |  |

 |

|  |
| --- |
| **C. Computers and Servers: Destruction of Requesting Organization Confidential Information Accessed, Used or Retained (For example, Desktop, Personal Computer, Laptop or File Server) Excluding Backup Systems** **Select one of:** |
| **** Not applicable - No storage on CD/DVD or Similar Portable Optical/Magnetic Disk |
| **** The following external service provider was contracted to complete secure destruction:

|  |
| --- |
|   |

Provide the name of the service provider in the space above and **append a copy of the certificate**.Provide the **title and date of the contract** between the Requesting Organization and the service provider.Note that the certificate must set out the date, time, location and method of secure destruction employed as well as the full name and signature of the operator completing the work. |
| **** Physical destruction and/or use of data destruction software by staff using the following method(s):*NOTE: Industry best practices for the secure destruction of data are constantly evolving and this is particularly true for data in electronic format. For general information with respect to secure destruction methods, please review the NIST Guidelines for Media Sanitization at* [*http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf*](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf)*. Sanitization techniques are outlined in Section 5.*

|  |  |  |  |
| --- | --- | --- | --- |
|  Degaussing |  |  |  |
|  Grinding (platters only) |  |  |  |
|  Incinerating |  |  |  |
|  Shredding |  |  |  |
|  Sanitizing Overwrites | Number of overwrites: \_\_\_\_ | Software used (including version): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  Selective Wipes | Number of wipes: \_\_\_\_ | Software used (including version): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **** | Briefly describe the selective wiping method, method of marking or tagging of Confidential Information that makes restoration impossible­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Please confirm the device(s) selectively wiped remain under the secure custody and control of our organization, and subject to the privacy and security policies of our organization. |
|   | Please confirm the device(s) selectively wiped is/are subject to an end-of-life policy that requires secure physical destruction, degaussing (where appropriate) or complete sanitizing overwrite of the entire device/media in accordance with industry best practices, prior to the media leaving our organization’s custody and control. |
| Location (Full Address): |  |
| Date (Month Day, Year): |  | Time (Hr:Min AM/PM): |  |
| Types of electronic data: |  |
| Full Name of Staff Completing Activity: |  |
| Title/Position of Staff Completing Activity: |  |
| Signature of Staff Completing Activity: |  |

 |

|  |
| --- |
| **D. Backup Systems and Media: Destruction of Requesting Organization Confidential Information Retained** **Select one of:** |
| **** Not applicable - No storage on CD/DVD or Similar Portable Optical/Magnetic Disk |
| **** The following external service provider was contracted to complete secure destruction:

|  |
| --- |
|   |

Provide the name of the service provider in the space above and **append a copy of the certificate**.Provide the **title and date of the contract** between the Requesting Organization and the service provider.Note that the certificate must set out the date, time, location and method of secure destruction employed as well as the full name and signature of the operator completing the work. |
| **** Physical destruction and/or use of data destruction software by staff using the following method(s):*NOTE: Industry best practices for the secure destruction of data are constantly evolving and this is particularly true for data in electronic format. For general information with respect to secure destruction methods, please review the NIST Guidelines for Media Sanitization at* [*http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf*](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf)*. Sanitization techniques are outlined in Section 5.*

|  |  |  |  |
| --- | --- | --- | --- |
|  Degaussing |  |  |  |
|  Grinding (platters only) |  |  |  |
|  Incinerating |  |  |  |
|  Shredding |  |  |  |
|  Sanitizing Overwrites | Number of overwrites: \_\_\_\_ | Software used (including version): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  Selective Wipes | Number of wipes: \_\_\_\_ | Software used (including version): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **** | Briefly describe the selective wiping method, method of marking or tagging of Confidential Information that makes restoration impossible­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Please confirm Backup Systems and Media are secure, subject to restricted access by a limited number of authorized personnel, and data found on backup systems are only utilized for business continuity and disaster recovery purposes. |
|   | Please confirm Backup Systems and Media containing **Requesting Organization** Confidential Information are subject to an end-of-life policy that requires secure physical destruction, degaussing (where appropriate) or complete sanitizing overwrite of the entire device/media in accordance with industry best practices, prior to the medial leaving our organization’s custody and control. |
| Location (Full Address): |  |
| Date (Month Day, Year): |  | Time (Hr:Min AM/PM): |  |
| Types of electronic data: |  |
| Full Name of Staff Completing Activity: |  |
| Title/Position of Staff Completing Activity: |  |
| Signature of Staff Completing Activity: |  |

 |