**Department Name:** Information Technology Department

**Title:** Data Destruction Policy #2016-CISO-1

**Effective Date:** November 1, 2016

**Approved by:** Vice President of IT and Chief Information Officer

**Overview:**

A+ Corporation (hereinafter “A+” or the “Company”) conducts background checks on behalf of companies, government agencies, and other organizations that have chosen to outsource their pre-employment screening function, and credit checks for Lessees and Landlords to assist with their evaluation of the financial fitness of prospective tenants and Lessees. In this capacity, A+ is entrusted with highly sensitive information. A+ has spent a considerable amount of time and money, and has devoted significant resources towards developing solid customer relationships and proprietary software to meet their needs. The Fair Credit Reporting Act requires A+ to safeguard its customer’s confidential information, and imposes severe penalties for divulging such information for unauthorized purposes.

**Purpose:**

The purpose of this Policy is to define the requirements for disposal of physical records and Information Technology Equipment (hereinafter “ITE” or “equipment”) that has been used to collect, transfer, store or process private or restricted data and information as defined by the Company’s Data Classification Policy (also see **Appendix A**). Effective destruction practices will better enable A+ to protect the Company and its customers’ information assets from unauthorized access, use and disclosure.

**Scope:**

The Data Destruction Policy applies to all ITE that is owned or leased by A+ that is no longer supported by the vendor or reusable. Examples of ITE includes, but is not limited to hard drives, RAM, removable storage devices, back-up tapes, and printer/scanner/copy/facsimile machines (hereinafter “printers”). The Policy also applies to physical records that contain non-public Company, employee, or customer information. Physical records that contain public information only are not within the scope of this Policy.

All employees, contractors, vendors and other affiliates that handle A+ electronic information are required to comply with this Policy. Third party Service Level Agreements shall also be in compliance and aligned with the standard information and best practices dictated by this Policy.

**Roles and Responsibilities:**

The Vice President of IT and Chief Information Officer is responsible for approving this Policy and all subsequent revisions as are required and/or recommended by the Director of IT Security. Management is responsible for ensuring employees are properly trained on and that they comply with this Policy. IT Operations is responsible for disposing of unusable equipment in accordance with this Policy. IT Audit will monitor compliance and report Policy infractions to the Chief Compliance Officer. All employees, contractors and affiliates are required to comply with this Policy.

**Policy:**

A+ shall dispose of private and restricted Company, employee and customer information and data in a manner that prevents unauthorized access, use or disclosure.

Computer and printer hard drives, RAM, removable storage devices, and back up tapes shall be disposed of using technologies that perform a series of successive data writing and erasing in random patterns and low level formatting that ensures the electronic data is completely irrecoverable.

If the equipment is no longer usable, A+ will engage a third party vendor to physically destroy the magnetic media in a manner that is commensurate with the sensitivity defined by the Data Classification Policy and depicted in the Data Destruction Matrix (see **Appendix B**).

All physical records that contain private or restricted information that is required to be stored in accordance with the Data Retention Policy shall be disposed of in designated, locked shred bins. A+ will similarly engage a third party vendor to empty and shred documents in the bins as depicted in the Data Destruction Matrix.

Certificates of destruction shall be retained from all third party vendors who destroy equipment or physical records on behalf of A+ corporation in accordance with the Data Destruction Matrix.

**Policy Compliance:**

IT Audit will monitor Policy compliance through various methods, including Whistleblower Hotline calls, business tool reports, internal and external audits, and Management feedback.

**Enforcement:**

Any employee (including part-time employees and consultants), contractor, vendor or other third party who willfully violates this policy may be subject to disciplinary action (up to and including termination), legal action or sanctions.

**Related Policies and Procedures:**

Data Classification Policy v4.1

Data Retention Policy v2.1

Whistleblower Policy v2.3

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Effective Date** | **Author** | **Change Summary** |
| 2016-CISO-1  | November 1, 2016 | Director of Information Security | Policy Implemented |
|  |  |  |  |
|  |  |  |  |

**Appendix A – Excerpt from Data Classification Policy**

|  |  |
| --- | --- |
| **Data Classification**  | **Description** |
|  Public | Unauthorized use or disclosure of Public data or information presents negligible risk to Company and/or its customers. |
| Private | Unauthorized use or disclosure of Private data or information presents a moderate level of risk to the Company and/or its customers. |
| Restricted | Unauthorized use or disclosure of Restricted data or information presents a significant level of risk to the Company and/or its customers. |

**Appendix B – Data Destruction Matrix**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Classification / Medium** | **Hard Drives** | **Removable Storage Devices** | **RAM** | **Back Up Tapes** | **Printers** | **Physical Records** |
| **Public** | 1, 2 | 1 |  | 2 | 1, 2  | N/A |
| **Private** | 1, 4 | 1 | 4 | 2 | 1, 2, 4 | 5 |
| **Restricted** | 1, 3, 6 | 1, 3, 6 | 3, 6 | 1, 2, 3, 6 | 1,3, 6 | 3, 6 |

|  |
| --- |
| **Minimum Destruction Requirements** |
| 1 | Wipe/Clean (USB) |
| 2 | Reimage/Overwrite (tape) |
| 3 | Off-site destruction |
| 4 | On-site destruction |
| 5 | On-site shredding |
| 6 | Certificate of Destruction required |