Disposal and Destruction Policy: Equifax Corporation

Dawn M. Inman

CYB-348-Z1

Disposal and Destruction Policy: Equifax Corporation

Policies are an essential tool because they provide the guide that helps any organization move toward their goals and objectives. (PCG, 2019) Policies are a formally agreed upon high-level principles and requirements that an organization, department or area of the business must follow and they set the directional tone for the area they are written for. (Amadei, 2016) Policies can identify key activities that take place in the organization as well as the small, seemingly insignificant issues such as building rules, children, pets, smoking, or parking. Policies are also a guide for handling issues that happen when the policies are not followed or new issues arise. (CMHC, 2018)

Having a company-wide Disposal and Destruction Policy before the Equifax data breach could have reduced one issue that was brought against them in court according to a staff report by an investigative subcommittee of the U.S. Senate. During the time of trying to mitigate the data breach, Equifax kept its interoffice communications set on a delete mode. This made it impossible for investigators to look at everything Equifax did to work toward mitigation, which likely cost them millions because their mitigation steps were lost. (U.S. Senate, 2018) Part of a disposal and destruction policy is also document and information preservation, evaluating what information and devices should be sanitized and what should be retained and transferred elsewhere. (NYU, 2019). It also includes deleting data from devices, overwriting and destruction and can include paper sources and hardware. (CISA, 2019)

# Objective

To develop a policy for regulation of disposal and destruction of information resources including data, paper products and hardware, specifically applying the policy to the Equifax Corporation.

## Results and Analysis1

According to the SANS templates, the process of developing a disposal and destruction policy requires looking at these distinct areas: Overview, Purpose, Scope, Policy, Policy Compliance, Related Standards, Policies and Processes, Definitions and Terms and a Revision History. (SANS, 2014)

The process for Equifax could also include: How to Store Sensitive Documents, Physical document destruction and How to choose a Document Destruction Company. (James, 2018)

**Possible Disposal and Destruction Policy for Equifax Corporation**

**Overview**

Information can be stored in different forms and use different methods. All forms of information storage need to be properly disposed of at the end of the usable period of the information life. Technology equipment contains parts that could cause security issues if it is simply thrown away. Paper information could be used in a malicious manner if sensitive information is disposed of using standard common methods. Special care must be taken in both instances to ensure the complete removal of all information from the access of anyone who could happen across it. (SANS, 2014)

**Purpose**

The purpose of this policy is to provide guidelines for the disposal of paper information, data information and technology equipment owned by the Equifax Corporation. (SANS, 2014)

**Scope**

This policy is to be applied to all out of date paperwork, any and all papers with sensitive information, client or other affiliate information as well as corporate information and private documents. It also applies to all equipment owned or used by the company like computers, tablets and smart phones but also including internet of things items such as keyboards, mice, speakers, printers, scanners, typewriters, some wall plugs and appliances with WIFI access and any other internet of things items that have network access.

All Equifax Company employees and affiliates are expected to adhere to policy compliance. (SANS, 2014)

**Policy**

1. Paper and Hard Copy Disposal of Information:
2. Documents can be compromised if left to pile up inside an office or unsecure environment. Confidential and sensitive information needs to be secured daily while inside the office insuring that sensitive documents do not fall prey to unexpected circumstances. Locked collection containers purposed for shredding are ideal.
3. Set up a weekly or bi-weekly routine for document disposal keeping in mind what amount of paperwork needs to be secured daily, making sure locked containers do not become overfull causing sensitive documents to remain out in the open.
4. Use a AAA NAID certified company for hard copy disposal.
5. Include non-paper media in the disposal program. These can include CD’s, DVD’s, and backup tapes. (Richards & Richards, 2019)
6. Destruction and Disposal of Data, Information Systems and Other Technology.
7. Electronic devices include but are not limited to:

* Computers, Smartphones, Tablets and Networking Equipment including any device that can store and/or process data.
* External Hardware and Peripherals including printer, monitors, external hard drives.
* Digital Media like cameras, T. V’s both smart and regular, media players, etc.
* Gaming consoles which can be electronic, digital or computer devices which use a video signal or image for video gaming.
* Any Internet of Things items such as coffee pots, refrigerators, Alexa units, WIFI wall plugs or any device that has internet access which is used to run, function or help those using them.

1. Technology assets are to be sent to Equipment Disposal for proper disposal.
2. Equipment will be assessed, making sure all information that needs to be recouped is either securely moved to another device or securely stored.
3. Equipment will have all data, files, software and operating systems completely removed from the equipment using disk sanitizing software. This software has the requirement of overwriting all disk sectors with zero-filled blocks which meets the Department of Defense standards.
4. No computer or technology is to be sold, given away, disposed of via skips, dumps or landfill or used in any manner once it has been established to be at the end of life.
5. Electronic drives will be degaussed or overwritten with a commercially available disk cleaning program. Drilling, crush, shredding or other demolition methods are acceptable for making hard drives unreadable. Complete destruction of the unit is preferred by removing and destroying the memory and storage devices inside the machine.
6. Once the device has been completely wiped it will be marked with a sticker stating the wipe and the technician information. (SANS, 2014)

**Policy Compliance**

Compliance to this policy will be reported back to the Equifax CISO via the reporting of the Information Security (Infosec) Team. These reports can include but are not limited to internal and external audits, feedback and business tool reports.

All exceptions to the policy need to be approved in advance through the Infosec team.

Disciplinary action will be taken if any employee is found in violation of this policy, up to and including termination. (SANS, 2014)

**Related Standards, Policies and Processes**

NAID- https://naidonline.org/

PRISM- https://prismintl.org/

CISA Standards- https://www.us-cert.gov/ncas/tips/ST18-005

**Definitions and Terms**

None

**Revision History**

List below any revisions to the Disposal and Destruction Policy, the dates and Committee or Company group whom created the changes in the policy.

### Conclusion.

The objective to the lab was met, as a simple policy for disposal and destruction of paper and technology hardware and software was created, using a SANS technology equipment disposal policy as a rough guide. From there the student looked at several different references to create a new policy that could apply to the Equifax corporation. Using a policy like the one created can help Equifax to keep its information secure. This would avoid issues that other companies have had with sensitive papers falling into the street which created a compromise resulting in severe data loss to hackers. Computers and hardware have also been found in dumps that still have all of the sensitive information on them instead of securely wiped and destroyed. These are situations that Equifax needs to avoid, specifically after the Data breaches it has already had. This lab provided the student with an excellent foundation for the end of life of various types of information that can be used at future employment or when helping businesses with security issues.

References

Amadei, Lauren. (November 1, 2016). *Why policies and procedures matter*. Risk Management. Retrieved December 8, 2019 from http://www.rmmagazine.com/2016/11/01/why-policies-and-procedures-matter/

CISA. (November 14, 2019). *Security tip (ST18-005): Proper disposal of electronic devices.* Retrieved December 8, 2019 from https://www.us-cert.gov/ncas/tips/ST18-005

CMHC,Canada Mortgage and Houseing Corporation. (March 31, 2018). *Why are policies important.* CMHC School. Retrieved December 8, 2019 from https://www.cmhc-schl.gc.ca/en/maintaining-and-managing/managing-affordable-housing/housing-management-hub/policy-information/why-are-policies-important

James, Mike. (July 6, 2018). *GDPR and physical document deletion: Four things you need to know.* Global Sign. Retrieved December 8, 2019 from https://www.globalsign.com/en/blog/physical-document-deletion-gdpr/

NYU. (2019).  *Policy: Standard for destruction and disposal of electronic equipment and data.*  Retrieved December 8, 2019 from https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/standard-for-destruction-and-disposal-of-electronic-equipment-an.html

PCG, Pacific Crest Group. (2019). *Are your policies and procedures a barrier to growing your company?*  Retrieved December 8, 2019 from https://www.pcg-services.com/are-your-policies-and-procedures-a-barrier-to-growing-your-company/

Richards & Richards. (2019).  *4 ways to tune up your document disposal program.* Retrieved December 8, 2019 from https://www.richardsandrichards.com/4-ways-to-tune-up-your-document-disposal-program/

SANS. (2014). *Technology equipment disposal policy.* Consensus Policy Resource Community. Retrieved on December 8, 2019 from https://www.sans.org/security-resources/policies/server-security/pdf/technology-equipment-disposal-policy

U.S. Senate. (2018).  *How Equifax neglected cybersecurity and suffered a devastating data breach.* Committee on Homeland Security and Governmental Affairs. Retrieved December 8, 2019 from https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf