# EAS Security Best Practices for Archivists

## Draft: July 31, 2014, Skip Kendall

### Introduction

This document contains discussions of the application of Harvard security policies. While every effort will be made to keep this document current, archivists should not consider this document authoritative on current security requirements. Rather, they should be familiar with Harvard’s security levels and their requirements. Throughout the document, the word “archivists” is used to refer to curatorial staff. However, this document should also be understood to apply to special collection librarians using EAS to process personal archives.

General Discussion of Email  
In general, email is classified as level 3 in Harvard’s data security classification table, defined as “information that could cause risk of material harm to individuals or the University if disclosed.” The only likely exceptions to this are

* collections that are publicly available, such as public mailing lists, which would likely fall under level 1, and
* collections with highly sensitive data, which would likely fall under level 4, defined as “Information that would likely cause serious harm to individuals or the University if disclosed.”

Level 3 information requires secure storage at all times, primarily meaning that Harvard repositories should store it on encrypted drives or within secure networks. If the email is to be transferred on a portable device prior to deposit in EAS, the content should be protected against access if the device is lost or stolen. In practice, this means the content should be encrypted.

### Sensitive Content

Some forms of sensitive content, such as credit card numbers, will be discovered by the automated screening conducted upon ingest. Other forms may be discovered through contextual means, such as knowing what kinds of sensitive conversations the donor might have engaged in. No matter the form of the sensitive content, care should be taken to use metadata or other methods to mark it. EAS batch functionality allows metadata to be applied to many messages at once based on relatively complex search criteria, providing a way to mark messages that may have sensitive content.

### Donor Communications

As with all donations or archival transfers, donors should be aware of the repository’s intentions regarding their e-mail. Archivists should be prepared to discuss the security of transfer procedures, access restrictions and intentions, and the location of liability for any content accessed by unauthorized personnel. Archivists should also acquire as much information as possible about sensitive content from the donor. For example, donors may be able to identify folders likely to contain such content. Donors can also help determine if level 4 information is present.

### Internal Security

Curatorial staff with access to EAS should be aware of security issues. Such staff should be required to acknowledge their duty to protect sensitive content through the Confidentiality Agreement available in PeopleSoft or an equivalent agreement. Staff should also, as a general practice when EAS is open, lock their computer whenever leaving their desk.

### Unauthorized Access

In the event of unauthorized access to the EAS servers, i.e. a security breach, Harvard may be required to contact individuals affected. While maintaining donor contact information is standard archival practice, this requirement underscores the need to do things properly. Knowing the location of sensitive content will also help in case the notification of more than donors is required.

### Post-EAS

After transfer to DRS, archivists may need to download EAS-processed content. Care should be taken with sensitive content as well as content where the sensitivity is unknown. Archivists should also be aware that the section of this document on unauthorized access also applies to unauthorized access to the DRS servers.