# 1100 Electronic Records Management Policy v2

## 1100 ELECTRONIC RECORDS MANAGEMENT POLICY

---

### 1100.1 Purpose:

The purpose of this Electronic Records Management Policy is to establish guidelines and procedures for the backing up certain electronic records, as well as the retention and destruction of
any such backup by the Archdiocese of Baltimore.

### 1100.2 Scope:

This Policy applies to electronic records that are stored on computer servers owned, leased, or provisioned at third-party hosting facilities and maintained or managed by the Archdiocese of Baltimore technology department.

### 1100.3 Electronic Records are Archdiocesan Property:

All electronic records generated or received by the Archdiocese are the property of the Archdiocese. Employees do not have any personal or property rights to records, electronic or otherwise, created, received, or generated on behalf of the Archdiocese. Similarly, no third party storage facility or entity has any personal or property rights to records, electronic or otherwise, stored by the Archdiocese at or with any such facility or entity.

## 1100.4 Definitions:

### 4.1. Electronic Record

An Electronic Record includes recorded information, regardless of medium or characteristic, which is stored on a physical or virtual computer server owned or leased maintained by the Archdiocese.

### 4.2. Records Hold

A Records Hold is the cessation of destruction of any records that relate to the subject of the Records Hold.

### 4.3. Backup

A Backup, or the process of backing up, refers to the copying and archiving of computer data for later retrieval.

## 1100.5 Backup and Retention:

### 5.1 Enforcement and Implementation

The Director of Information Technology is responsible for creating, updating, and implementing this Policy.

### 5.2 Backup creation and maintenance

The Division of Information Technology will ensure that Backups of Electronic Records are maintained and purged in accordance with this Policy.

### 5.3 Records hold

A Records Hold is necessary following the initiation or anticipated initiation of governmental or regulatory investigations and administrative or legal proceedings regarding the Archdiocese and/or its officers, directors, agents, or employees.  In the event any employee learns of any proceeding or anticipates the initiation of a proceeding, he or she should immediately inform the Division Director, who should then immediately contact the

Director of Information Technology and Archdiocesan Legal Counsel to initiate a Records Hold.

## 1100.6 Destruction of Backup Storage:

### 6.1 Periodic Destruction:

Except where a Department/Division formally adopts a longer retention period, all Monthly Backups should be purged in accordance with this Policy.

### 6.2 Ensuring Litigation Hold is not in Place Prior to Destruction:

The Director of Information Technology is responsible for ensuring that a Monthly Backup is not subject to a Records Hold prior to destruction.

### 6.3 Three-Year Destruction Schedule:

A Monthly Backup that has been retained for at least three (3) years since its creation should be purged using appropriate electronic data destruction procedures, except that a Monthly Backup for the month of December should not be purged.

### 6.4 Destroying Existing Monthly Backups:

Any Monthly Backups in existence as of the effective date of this Policy that were created more than three (3) years earlier should be purged using appropriate electronic data destruction procedures, with the caveat that a Monthly Backup for the month of December should not be purged.

### 6.5 Retained Records:

Absent a Records Hold, ordinary implementation of this Policy should result in the following Monthly Backups being retained: 1) those less than three years old and 2) Monthly Backups for the month of December (regardless of age).