GENIUS PROGRAMS

My Food PROGRAM | Ready RECORDS

Updated September 4, 2024

INTRODUCTION

My Food Program (MFP) and Ready Records (RR) are products of Genius Programs LLC and collect information about sponsoring organizations, their sites, and the participants in the USDA Child and Adult Care Food Program and Summer Food Service Program. We need to gather this information in order to meet the Federal and State recordkeeping requirements. However, this information needs to be kept away from persons who are not authorized to access that information.

This document summarizes how MFP secures data for its customers. It is intended for non-technical audiences. The summary applies to the MFP and RR web sites. It also describes how data is secured by the corresponding MFP and RR mobile applications. For the purposes of this overview, the term MFP covers both My Food Program and Ready Records. The term “food programs” covers the USDA Child and Adult Care Food Program, including the At-Risk Afterschool Meals Component and the USDA Summer Food Service Program.

MY FOOD PROGRAM DATA SECURITY PROGRAM

A Data Security program needs to ensure the following three things:

1. **Confidentiality** – data is disclosed to only persons who should see that data.
2. **Availability** – data needs to be accessible to be useful to MFP customers.
3. **Integrity** – data that has been entered by users has not been tampered with by users or administrators of MFP.

CONFIDENTIALITY

MFP applies a variety of safeguards to ensure that data remains confidential. Confidentiality applies to both customer and participant data.

Physical Security

Data is stored in data centers run by a major cloud computing provider known as Amazon Web Services (AWS). AWS provides physical security controls that restrict access to the computers used to run MFP. AWS physical security controls are audited regularly by third-parties and have been verified to meet standards required by the payment card industry and national standards bodies.

continued on next page >

Encryption

MFP data is encrypted both in transit and at rest. Data entered into MFP is encrypted using industry standard encryption techniques. These same techniques are used to secure banking information and credit card information as it is transmitted over the public internet. Once data arrives at the servers used by MFP, it is encrypted as it is entered into the database.

Identity and Authentication

MFP restricts access to data based on the login information provided by the site or sponsor.

System administrators must employ multiple factors to access system resources. In addition, system administrator access requires a secret key rather than a password for authentication.

AVAILABILITY

Data needs to always be available in order to meet the recordkeeping requirements of the food programs. MFP uses the following measures to make sure data is available.

Servers and Networks

MFP systems are located in AWS' computing cloud. AWS' computing cloud is designed to provide highly available and reliable computing resources, disk space, and networking infrastructure. These servers are physically secure and AWS customer's machines are separated from each other. However, it is up to MFP's team of system administrators to configure and use these systems securely. MFP's system administrators regularly scan the servers and networks for potential security issues and regularly review network configuration for security problems.

MFP only utilizes AWS systems in the United States. No data is stored in off-shore locations.

Backups

All computing infrastructure can fail. And human error can remove or tamper with data. MFP backs up data stored in the system using a variety of industry standard techniques. These techniques provide both a "cold" backup and a backup to the point where a failure or error occurred. Backups are taken daily and stored in multiple locations within AWS' infrastructure. Recovery procedures are regularly tested to ensure the backups are valid.

Disaster Recovery

While it is unlikely, it is possible for AWS servers to become unavailable. AWS has computing infrastructure located in several US-based data centers. MFP has redundant computing systems located in geographically dispersed data centers within the United States. In the event AWS servers are not available in the primary region, a backup region can be started to ensure that MFP is available for use by its customers.

continued on next page >

INTEGRITY

Ensuring that data is reliable and has not been tampered with is crucial to using MFP to monitor and run the food programs.

Keeping Hackers Out

MFP employs a variety of techniques to ensure that hackers do not steal or obscure data. These techniques include:.

- Constant monitoring of network traffic
- Blocking access to computers from the public internet and each other unless needed.
- Monitoring of servers for software that needs to be updated for security issues.
- Monitoring of servers to ensure that files have not been tampered with.

Multi-tenancy

MFP is a multi-tenant system. This means that multiple MFP customers are sharing the computers used to provide MFP. Consider this analogy to understand what this means.

MFP is like a cluster of apartment buildings. Each apartment building (sponsor) has one or more apartments (sites). One site's users can't see another site's data much like a tenant in an apartment building can't go into another tenant's apartment. Sites have their own access to MFP for the site's users. Sponsors can see a site's data. Sponsors are like the building maintenance persons for apartments. They can see all apartments to do their jobs. However a sponsor can't access another sponsor's data..

Audit Trail

All access to MFP by users and system administrators is logged to a centralized server. In the event of malicious activity, the audit trail can reveal who accessed a system, when that access was done, and what the user did.

In addition, changes to database data is tracked by MFP automatically. This tracking allows MFP's support team to understand how a particular record was changed, who did the change, and when that change happened.

CONCLUSION

MFP works diligently to ensure that your participant's data is kept away from hackers and that MFP is available to use. We take the responsibility of taking care of your data seriously.