Frequently Asked Questions about Scanning of Publicly-facing Folders on IS&T-supported File Storage Systems

Frequently Asked Questions about Scanning of Publicly-facing Folders on IS&T-supported File Storage Systems

Why is this important?

Keeping sensitive data safe from inappropriate access and accidental disclosure is of utmost importance to MIT and our community. Inadvertent disclosure of regulated data periodically happens through improper permissions. Some information that is considered sensitive data requires special care and handling. Inappropriate handling of the data could result in penalties, identity theft, financial loss, invasion of privacy, or unauthorized access by an individual or many individuals. Our proactive scanning of publicly exposed files is intended to help protect our community from these events.

You can find out more about how to protect MIT, as well as your own personal data, here: http://infoprotect.mit.edu/

What kind of information is regulated?

Regulated data includes Protected Health Information (PHI), social security numbers, student education records, financial account numbers, and data subject to United States export control or trade embargo regulations. To find out more about data protection and classification at MIT, please visit http://infoprotect.mit.edu/what-needs-protecting

What does publicly-facing mean?

In this case, it means that the file or folder security settings are set to public instead of private. For MIT AFS this means directories that have system:anyuser OR system:authuser read or higher permissions granted.

How can I protect my data?

Set your file or folder security to private, and don't store regulated information on AFS, Dropbox, or OneDrive systems. Learn more about how to protect your personal data here: http://infoprotect.mit.edu/your-personal-data

What happens if regulated data is discovered through a scan?

IS&T will consult Office of General Counsel and reach out to the owner to have the information removed from the publicly-facing folder.

What are the guidelines for information stored by users within IS&T-supported systems?

You can find out more information on our Knowledge Base about best practices for storing information while using these systems.

What content-scanning and data-loss-prevention tools are being used?

IS&T is using a custom tool for AFS scanning.

When did these scans begin, or when will they start?

Currently, daily scans of AFS are taking place.

If I have questions or concerns about this practice, who should I contact?

If you have any questions, please contact, John Charles, VP IS&T at jcharles@mit.edu.