Incydr Gov Key Compliance Features

While security regulations may differ in scope and complexity, they all build off of basic information security best practices. It's in these foundational controls that Incydr Govs Incydr Gov provides the greatest support in reaching your compliance obligations:

Insider Threat Protection

- Detect when users move files to removable media, web browsers/applications and cloud sync folders
- Identify files that are shared externally via corporate OneDrive, Google Drive and Box accounts
- Define alert criteria based on user, data exfiltration vector and file count or size
- Monitor and alert on use of removable media and portable storage devices

Detection and Response to Incidents

- Security teams can review event activity in seconds, even when user devices are offline
- All file activity is automatically indexed and made searchable to reduce the time it takes to detect and respond to insider threats

File Preservation

- Incydr Gov protects the confidentiality, integrity and availability of your data by preserving exact copies of files that can be restored
- Files and their respective metadata are encrypted before secure transmission to storage servers, where data remains encrypted at rest

Malware Protection

- Incydr Gov provides malicious code protection mechanisms on user endpoints
- Endpoint file preservation provides point-in-time recovery from malicious software

Encryption

- Incydr Gov protects the confidentiality and integrity of transmitted information and information at rest
- Communications between the Incydr Gov endpoint app and the storage servers are encrypted using AES 256-bit encryption
- Files and their respective metadata are AES 256-bit encrypted in the endpoint app and remain encrypted in storage servers

Audit/Logging

- Incydr Gov allows agencies to log file activity on user endpoints
- Incydr Gov generates audit records with the following event information:
    - Type
    - Date/time
    - Location
    - Source
    - Outcome
    - File involved
    - Identity of any individuals or subjects associated with the event

Incident Management

- Incydr Gov provides file activity and the ability to view endpoint files to support after-the-fact investigations of security incidents
- Incydr Gov allows for detailed analysis of user file movement activity on a device

Code42 is committed to helping organizations reach their compliance obligations. If you have additional questions about how Code42 can assist with your organizational compliance needs, please contact your Code42 representative today.

CODE42

Code42 is the leader in insider risk detection and response. Native to the cloud, Code42 rapidly detects data loss, leak, theft and sabotage as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider risk while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's insider risk solution can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity, NEA and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2020. For more information, visit code42.com, read Code42's blog or follow the company on Twitter. (OV2103244)