Compliance Standards

Executive Summary

DFS by DreamGRC is a cloud-based Digital Forensics as a Service platform that helps organizations conduct forensic investigations, incident response, and compliance activities. Designed for corporate security teams, law enforcement, and digital forensics experts, this platform combines industry-standard tools with advanced machine learning in a secure, compliant environment. This document outlines how DFS by DreamGRC meets and exceeds industry-recognized standards including NIST SP 800-86, GDPR, and ISO/IEC 27037:2012, ensuring digital evidence is handled with integrity, security, and in accordance with legal requirements.

Overview

DFS by DreamGRC implements multiple layers of compliance to ensure that digital evidence is handled according to best practices and legal requirements. Our platform processes various types of digital evidence including disk images, memory dumps, log files, network captures, and file system artifacts, while maintaining strict controls over personally identifiable information (PII) and sensitive data.

NIST SP 800-86 Compliance

The National Institute of Standards and Technology (NIST) Special Publication 800-86, "Guide to Integrating Forensic Techniques into Incident Response," provides a framework for handling digital evidence in a forensically sound manner.

How DFS by DreamGRC meets NIST SP 800-86 requirements:

1. Collection Process

- **Secure Evidence Acquisition**: Our platform implements secure methods for collecting evidence from various sources including disk images, memory dumps, and network traffic.
- **Chain of Custody**: Automatic documentation of who collected what evidence, when it was collected, and how it was transferred.
- **Data Integrity**: SHA-256 and MD5 hashing to verify evidence hasn't been altered during transfer or storage.
- **Collection Logging**: Comprehensive logs of all collection activities with timestamps and user identification.

2. Examination Process

- **File Type Analysis**: Automatic identification and classification of file types to determine appropriate examination methods.
- **Metadata Extraction**: Automated extraction of metadata from various file formats to provide context.
- **Tool Validation**: All integrated forensic tools are validated against known benchmarks to ensure accuracy.
- **Examination Workflow**: Step-by-step guided examination processes to ensure consistent handling.

3. Analysis Process

- **Correlation Engine**: Advanced machine learning algorithms identify relationships between evidence items.
- **Pattern Recognition**: Automated detection of common patterns in log files, user activities, and system events.
- **Timeline Construction**: Automatic creation of comprehensive event timelines across multiple evidence sources.
- **Anomaly Detection**: ML-powered identification of unusual patterns or behaviors within data sets.

4. Reporting Process

- **Standardized Reports**: Consistent formatting of findings to ensure clarity and completeness.
- **Evidence Linking**: All conclusions are linked directly to the underlying evidence.
- **Technical Translation**: Automated conversion of technical findings into plain language explanations.
- **Court-Admissible Format**: Reports meet legal standards for admissibility with complete process documentation.

GDPR Compliance

The General Data Protection Regulation (GDPR) establishes strict guidelines for handling personal data. Although forensic investigations may have specific exemptions, DFS by DreamGRC implements GDPR principles to ensure that personal data is handled appropriately.

How DFS by DreamGRC addresses GDPR requirements:

1. Data Protection Principles

- **Data Minimization**: Tools to identify and isolate personal data to ensure only relevant information is processed.
- **Purpose Limitation**: Case-based data organization ensures evidence is only used for its intended investigation purpose.
- **Storage Limitation**: Configurable retention policies to ensure data is not kept longer than necessary.

2. Data Subject Rights

- **Access Controls**: Role-based permissions system restricts access to evidence based on user authorization levels.
- **Data Isolation**: Ability to segregate personal data from other forensic evidence when needed.
- **Processing Records**: Comprehensive audit trail of all processing activities involving personal data.

3. Security Measures

- **Encryption**: End-to-end encryption for data at rest and in transit.
- **Access Control**: Multi-factor authentication and granular permission settings.
- **Activity Monitoring**: Real-time logging of all user interactions with sensitive data.
- **Vulnerability Management**: Regular security assessments and updates to protect against emerging threats.

ISO/IEC 27037:2012 Compliance

ISO/IEC 27037:2012, "Guidelines for identification, collection, acquisition, and preservation of digital evidence," establishes international standards for digital forensic processes.

How DFS by DreamGRC implements ISO 27037 principles:

1. Evidence Identification

- **Automated Discovery**: Intelligent scanning to identify potential sources of digital evidence.
- **Classification System**: Categorization of evidence by type, relevance, and potential evidentiary value.
- **Priority Assessment**: Tools to determine which evidence sources should be processed first based on volatility and importance.

2. Evidence Collection

- **Remote Collection**: Secure agent-based collection capabilities for distributed environments.
- **Write Protection**: Enforcement of read-only access to preserve original evidence.
- **Collection Validation**: Automatic verification that collection methods maintain evidence integrity.

3. Evidence Acquisition

- **Forensic Imaging**: Creation of bit-by-bit copies of digital media with verification.
- **Memory Capture**: Live memory acquisition with minimal system impact.
- **Network Traffic**: Packet capture with filtering capabilities to focus on relevant communications.
- **Acquisition Logs**: Detailed documentation of all acquisition parameters and results.

4. Evidence Preservation

- **Immutable Storage**: Evidence is stored in a tamper-evident format to prevent modification.
- **Integrity Verification**: Regular hash validation to ensure evidence remains unchanged.
- **Access Logging**: Complete record of who accessed evidence, when, and for what purpose.
- **Secure Backup**: Automated backup mechanisms to prevent data loss.

Exceeding Basic Requirements

DFS by DreamGRC goes beyond minimum compliance requirements with additional features that enhance the forensic integrity and analytical capabilities of the platform:

Advanced Features that Enhance Compliance

1. Machine Learning Capabilities

- **Intelligent Correlation**: Automatically identify connections between evidence that might be missed through traditional analysis.
- **Anomaly Detection**: ML algorithms that identify unusual patterns or behaviors within evidence datasets.

- **Classification Optimization**: Self-improving algorithms that become more accurate as they process more evidence.

2. Forensic Storytelling

- **Narrative Construction**: Transforms technical findings into comprehensive stories that explain the evidence.
- **Visual Timeline**: Interactive chronological representation of events across multiple evidence sources.
- **Relationship Mapping**: Graphical representation of connections between evidence items, events, and entities.

3. Continuous Compliance Validation

- **Automated Checks**: Regular system tests verify that all components maintain compliance with relevant standards.
- **Tool Verification**: Validation of tool outputs against known benchmarks to ensure analytical accuracy.
- **Process Monitoring**: Continuous assessment of workflow adherence to forensic best practices.

4. Expert System Integration

- **Tool Orchestration**: Seamless integration with validated external forensic tools.
- **Recommendation Engine**: Intelligent suggestions for next investigative steps based on evidence characteristics.
- **Knowledge Base**: Incorporation of forensic best practices into workflow guidance.

Compliance Verification and Auditing

DFS by DreamGRC includes built-in features to verify and demonstrate compliance with relevant standards:

1. Compliance Reporting

- Generate detailed compliance reports showing adherence to NIST, GDPR, and ISO standards
- Document all security and privacy measures implemented in the platform
- Produce audit-ready documentation of evidence handling procedures

2. Process Validation

- Independent verification of forensic tool results
- Cross-validation of findings using multiple analytical methods
- Comprehensive logging of all validation checks and results

3. External Audit Support

- Detailed activity logs suitable for external compliance review
- Transparent system architecture documentation
- Regular penetration testing and security assessments

Conclusion

DFS by DreamGRC is built from the ground up with compliance at its core. By implementing and exceeding the requirements of NIST SP 800-86, GDPR, and ISO/IEC 27037:2012, our platform ensures that digital evidence is handled in a manner that is forensically sound, legally defensible, and respectful of privacy concerns.

Our commitment to compliance is not just about meeting minimum standards but about establishing a new benchmark for digital forensics platforms in terms of integrity, security, and analytical capability.

Data Types & Classification

DFS by DreamGRC is designed to handle diverse types of digital evidence while maintaining appropriate security controls for each data classification:

Types of Data Processed

- **File System Artifacts**: Directory structures, file metadata, allocation tables
- **Application Data**: Logs, databases, configuration files
- **Communication Records**: Email, chat logs, network traffic
- **System Memory**: RAM dumps, page files, hibernation files
- **Storage Media Images**: Complete disk images, partition data
- **User Data**: Documents, spreadsheets, presentations
- **Personally Identifiable Information (PII)**: When present in evidence

Data Classification & Handling

Each type of data is automatically classified according to sensitivity: - **Standard Evidence**: Basic metadata, system logs, non-sensitive files - **Sensitive Evidence**: Authentication data, encrypted content, proprietary information - **Regulated Data**: PII, financial information, health records - **Legal Hold Data**: Evidence subject to specific legal preservation requirements

Data Privacy & Retention

Privacy Controls

- **Data Minimization Tools**: Automated PII identification and extraction capabilities to isolate sensitive information
- **Access Tiering**: Granular permissions ensure users only see data relevant to their role and case assignment
- **Pseudonymization Options**: Tools to replace direct identifiers with pseudonyms while preserving analysis capabilities
- **Privacy Impact Assessment**: Built-in workflows to assess privacy implications of forensic activities

Retention Policies

- **Case-Based Retention**: Evidence retention tied to case lifecycle with configurable timeframes
- **Automatic Expiration**: Configurable policies for automatic deletion of data after defined periods
- **Legal Hold Management**: Override capabilities for evidence subject to legal preservation requirements
- **Selective Deletion**: Tools to remove specific data elements while preserving chain of custody records
- **Audit Trails**: Complete documentation of all retention decisions and deletion activities

Security Architecture

The DFS by DreamGRC platform implements a defense-in-depth security architecture:

DFS Security Architecture

Key Security Components

1. **Authentication Layer**: Multi-factor authentication, role-based access control
2. **Application Layer**: Input validation, secure coding practices, vulnerability management
3. **Processing Layer**: Sandboxed analysis environment, job isolation
4. **Storage Layer**: Encryption at rest using AES-256, secure object storage
5. **Network Layer**: TLS 1.3 encryption in transit, network segmentation
6. **Monitoring Layer**: Real-time intrusion detection, anomaly monitoring

Compliance Resources

- NIST SP 800-86 Standard - Guide to Integrating Forensic Techniques into Incident Response

- NIST SP 800-171 - Protecting Controlled Unclassified Information
- GDPR Official Text - General Data Protection Regulation
- ISO/IEC 27037:2012 - Guidelines for identification, collection, acquisition, and preservation of digital evidence
- ISO/IEC 27001:2022 - Information security management systems