tyco Security Products

White Paper for Security Professionals

21 CFR Part 11

Field Level Audit Trail and Strong Password Protection

What does a security system have to do with a federal regulation like 21 CFR Part 11? Plenty.

The FDA guidelines set forth the rules for acceptability and use of electronic records and signatures in lieu of “paper” records and “handwritten” signatures. That includes all personnel records in your security system.

So, how do you ensure that all security clearance changes, expiration date modifications, and new administration privileges are tracked to the FDA standard? And, how do you ensure that only authorized personnel can make those changes in the first place?

C•CURE 800 and C•CURE 9000 field-level audit trail and domain password protection

Overview

Signed into law in 1997, 21 CFR Part 11 is a United States Food and Drug Administration (FDA) regulation that affects all pharmaceutical companies, medical device manufacturers, and other entities who create, modify, transmit, receive, and store data that is governed by the FDA. The scope of the regulation includes requirements for legally storing, transmitting, and verifying electronic signatures. It also specifies required conditions needed to maintain the integrity of electronic data stored and modified on computer systems.

Data Validation Capabilities Required by Part 11

The ability to verify the integrity of data stored on computer systems is called data validation. The key regulations on this topic are found in Section 11.10, which requires organizations to "employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records" as follows:

- Section 11.10 (a) requires "Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records."
- Section 11.10 (d) requires "Limiting system access to authorized individuals."
- Section 11.10 (e) requires "Use of secure, computer-generated, time-stamped, audit trails" that, among other things, "shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying."

C•CURE 800 and C•CURE 9000 Features – How They Help

Field-level Audit Trail of Personnel Data

C•CURE 800 and C•CURE 9000 field-level audit trail provides a comprehensive assessment of any additions, deletions or modifications that have been made to personnel data in the C•CURE 800 or C•CURE 9000 security management system.

The following requirements have been met by C•CURE 800 and C•CURE 9000 field-level audit trail:

- Independently recorded
- Computer generated
- Date and Time Stamped
- All changes, which create, modify or delete
- Can not obscure previous data
- Retention for full retention period
- Availability for inspection and copying for FDA

12/34/98 14:22:15 Person King, Martin Luther modified by Smith, John {import} Expiration date changed from "11/22/1997" to "12/22/1998"

12/34/98 14:22:15 Person King, Martin Luther modified by Smith, John {import} Clearance 2 changed from "" to: "FRONT DOOR"

By providing time and date stamped records of all changes to the personnel data, this new feature addresses the requirements of Section 11.10e. The audit trail functionality is kept programmatically and cannot be altered by anyone, including the system administrator.

Enhanced Password Protection

In version 8.0 of C•CURE 800, which was released in early 2003, enhanced password protection was added to the application.

C•CURE 9000 offers domain authentication for all operators. This is a secure way to login into the network before you can access the C•CURE 9000 application. This feature moves the authentication process from C•CURE 800/C•CURE 9000 to the operating system and also provides tools for locking or terminating C•CURE 800/C•CURE 9000 applications when a station is left unattended.

When the C•CURE Enhanced Password Protection or Domain authentication feature is used in conjunction with the policy management system provided by the operating system, administrators can create highly secure systems that:

- Meet the demands of most applications that require extensive security
- Comply with organizational standards for computer security

By limiting system access to authorized individuals, this new feature addresses the requirements of Section 11.10d.

Conclusion

The FDA's intent with 21 CFR Part 11 is to ensure that the data stored and modified on a computer workstation is trustworthy. This is necessary because data that contains critical information must be reliable and authentic. This regulation is so important that the FDA may begin imposing very large fines to companies who fail to comply.

- Field-level Audit Trail in C•CURE 800/C•CURE 9000 helps to ensure the integrity of data by creating a detailed audit trail of all additions, modifications and deletions of personnel data.
- Enhanced Password Protection in C•CURE 800 and Domain authentication in C•CURE 9000 moves the authentication process from C•CURE 800/C•CURE 9000 to the operating system and also provides tools for locking or terminating C•CURE 800/C•CURE 9000 applications when a station is left unattended.

About Software House

Software House, part of Tyco Security Products, manufactures security and event management systems including the innovative C•CURE 9000. Combined with a suite of reliable controllers lead by the iSTAR Edge IP door control module, Software House technologies are among the most powerful in the industry. With a strong foundation that is both open and IT friendly, C•CURE 9000 allows customers to integrate seamlessly with critical security and business applications. C•CURE 9000 is ideal for security-critical applications including those in government, healthcare, education, finance, utilities, and commercial.

For more information on Software House products, 1-800-507-6268 www.swhouse.com