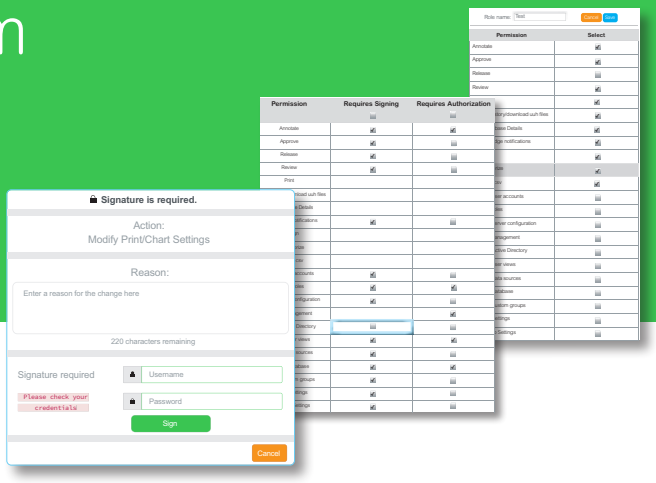
Data Reviewer Eurotherm FDA 21 CFR Part 11

(Opção com Audit Trail)



Eurotherm®

Especializada em Sistemas & Soluções, Serviços & Suporte

Otimize a Eficiência Operacional com Soluções Avançadas de Gerenciamento de Dados

Considerações sobre Conformidade Regulatória

Como parte do comprometimento contínuo para auxiliar na conformidade das Normas do Código Federal Americano do FDA (Food and Drug Administration) e especificamente com os requisitos do FDA 21 CFR Part 11, este datasheet demonstra como a experiência da Eurotherm ajuda os clientes a atender aos vários requisitos do FDA 21 CFR Part 11.

Cada subseção considerada é listada no cabeçalho das tabelas abaixo e as declarações de cada tabela são acompanhadas por um comentário demonstrando como a solução da Eurotherm auxilia na conformidade.

Sub Part B - Registros Eletrônicos

11.10 Controles para Sistemas Fechados	
(a) Validação de sistemas para assegurar precisão, confiabilidade, desempenho pretendido consistente e habilidade de discernir registros inválidos ou alterados.	A Eurotherm® oferece assistência na validação de produtos de acordo com as diretrizes do GAMP (Good Automated Manufacturing Process). Os dados originais são registrados em arquivos que estão em formato binário checksum proprietário da Eurotherm. Os detalhes não são publicados. A ferramenta de visualização rejeita registros inválidos / alterados (Ex. checksummed incorreta). Testes extensivos são realizados pela Eurotherm Ltd, uma empresa certificada ISO 9001. É possivel validar (e fazer a manutenção do status de validado) uma vez que as numerações de configuração e segurança são incrementadas cada vez que uma mudança é salva. Esses números são armazenados na trilha de auditoria.
(b) Habilidade em gerar cópias precisas e completas dos registros tanto em formulários eletrônicos em formato legível adequados para inspeção, revisão e cópia pela agência. As pessoas devem contatar a agência se houver questionamentos sobre a habilidade da agência em fazer tal revisão e cópia dos registros eletrônicos.	Cópias verdadeiras, precisas e completas na tela ou em impressões estão disponíveis através do Data Reviewer Eurotherm. As cópias eletrônicas verdadeiras, precisas e completas estão disponíveis copiando os arquivos de dados originais selecionando uma “impressora PDF” (requer Adobe Acrobat ou similar) para poder exportar gráficos no formato PDF.
(c) Proteção dos registros para habilitar sua recuperação imediata e precisa por todo período de retenção dos registros.	Os dados podem ser periodicamente extraídos do produto usando o Data Reviewer Eurotherm. Uma vez que os dados foram removidos do registrador, a estratégia de segurança e backup fica sob responsabilidade do usuário.
(d) Limitação do acesso ao sistema a pessoal autorizado	Contas de usuário protegidas por senhas individuais.
(e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora, para registrar independentemente a data e hora das entradas e ações do operador que criam, modificam ou excluem registros eletrônicos. As alterações nos registros não devem ocultar as informações gravadas anteriormente.Tal documentação de trilha de auditoria deve ser mantida ao menos pelo tempo exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.	Resistência a violações (incorporada no arquivo de histórico binário), trilha de auditoria gerada por computador e com registro de data e hora, incluindo reconhecimento de notificação, logins, detalhes de assinatura e alterações de configuração.

(f) Uso de verificações do sistema operacional para impor a sequência permitida de etapas e eventos, quando apropriado.	Se solicitado, uma segunda assinatura deve ser aplicada e ela também é registrada na trilha de auditoria.
(g) O uso de verificações de autoridade para garantir que apenas indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou dispositivo de entrada ou saída do sistema de computador, alterar um registro ou executar a operação em questão.	Contas de usuário protegidas por senha individual. Cada conta de usuário pode ter seu próprio conjunto de permissões ou privilégios para personalizar o que podem fazer na aplicação.
(h) Uso de verificações de dispositivo (ex. terminal) para determinar, quando apropriado, a validade da fonte da informação de entrada ou da instrução operacional.	Os eventos são registrados. O acesso à configuração do Data Reviewer é controlado e alterações feitas são registradas na trilha de auditoria.
(i) Determinação das pessoas que desenvolvem, mantêm ou usam sistemas de registros eletrônicos/assinatura para terem instrução, treinamento e experiência para realizar as tarefas para as quais foram designados.	De acordo com Procedimento.
(j) O estabelecimento e a adesão a políticas escritas que responsabilizem os indivíduos por ações iniciadas sob suas assinaturas eletrônicas, a fim de impedir a falsificação de registros e assinaturas.	De acordo com Procedimento. Porém, o Active Directory da Microsoft® pode ser utilizado para gerenciar procedimentos de login e senhas.
(k) Uso de controles apropriados sobre sistemas de documentação incluindo: **(1)** Controles adequados sobre distribuição, acesso e uso da documentação para operação e manutenção do sistema. **(2)** Revisão e procedimentos de controle de alterações para manter uma trilha de auditoria que documenta o desenvolvimento e a modificação seqüenciados no tempo da documentação do sistema.	De acordo com Procedimento em conformidade com as diretrizes do Gamp®5 e gerenciamento do arquivo de configuração checksum durante o controle de mudança.

11.30 Controles para sistemas abertos	
As pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, a integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de recebimento. Tais procedimentos e controles devem incluir os identificados na seção 11.10, quando apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital, para garantir, conforme necessário, sob as circunstâncias, autenticidade, integridade e confidencialidade dos registros.	O aplicativo é direcionado para uso em sistemas fechados. Com sistemas/procedimentos externos apropriados, o aplicativo pode ser usado em um sistema aberto.

11.50 Composição das Assinaturas	
Os registros de assinatura eletrônica devem conter informações associadas à assinatura que indiquem claramente: **(1)** O nome do assinante impresso; **(2)** A data e a hora em que a assinatura foi executada; **(3)** A justificativa (tal como revisão, aprovação, responsabilidade, ou autoria) associada à assinatura	Os registros de assinaturas contendo o nome impresso (ID do usuário), data, hora e justificativa são atribuíveis a uma pessoa. A justificativa inclui assinatura/autorização junto a um tipo automaticamente gerado (ex. “config” para uma mudança de configuração), mais uma nota adicionada pelo operador (designada como: anotação, aprovação, revisão, emissão).
(b) Os itens identificados nos parágrafos (a)(1), (a)(2) e (a)(3) desta seção devem estar sujeitos aos mesmos controles dos registros eletrônicos e devem ser incluídos como parte de qualquer registro em formato legível do registro eletrônico (como um display eletrônico ou impressão).	Nome (ID), intervalo de tempo e justificativa estão inclusos no arquivo histórico em formato binário.

11.70 Assinatura / Ligação do Registro	
As assinaturas eletrônicas e assinaturas manuais executadas para registros eletrônicos devem estar ligadas aos seus respectivos registros eletrônicos para assegurar que elas não possam ser extraviadas, copiadas, ou sequer transferidas para falsificar um registro eletrônico por meios comuns.	A manifestação da assinatura está inclusa no arquivo histórico em formato binário. Para sistemas híbridos, as impressões criadas através do Data Reviewer Eurotherm para assinatura à mão sempre contêm detalhes de intervalo de tempo que permitem a recriação a partir dos dados originais.

Sub Parte C – Assinaturas Eletrônicas

11.100 – Requisitos Gerais	
(a) Cada assinatura individual deve ser única para cada pessoa e não deve ser reutilizada ou redesignada para qualquer outra pessoa **(b)** Antes de uma organização estabelecer, atribuir, certificar ou sancionar a assinatura eletrônica de um indivíduo ou qualquer elemento dessa assinatura eletrônica, a organização deve verificar a identidade do indivíduo.	O Data Reviewer Eurotherm atende este requisito uma vez que as contas de usuário não podem ter o mesmo nome de usuário. As contas expiradas permanecem no sistema e estão definidas como “aposentadas”. O número de contas de usuário não é limitado no software. De acordo com Procedimento.
(c) Pessoas usando assinaturas eletrônicas devem, antes ou no momento do uso, certificar a agência de que as assinaturas eletrônicas no seu sistema, usadas na data de 20 de agosto de 1997 ou depois, pretendem ser legalmente lançadas de modo equivalente às assinaturas tradicionais feitas à mão. **(1)** A certificação deve ser enviada em papel e assinada à mão, para o Escritório de Operações Regionais (HFC-100), 5600 Fishers Lane, Rockville, MD 20857 **(2)** As pessoas que usam assinaturas eletrônicas devem, mediante solicitação da agência, fornecer certificação ou testemunho adicional de que uma assinatura eletrônica específica é juridicamente vinculada como equivalente à assinatura feita à mão.	De acordo com Procedimento.

11.200 Componentes e controles de assinatura eletrônica	
(1) Empregar pelo menos dois componentes de identificação distintos tais como código de identificação e senha. **(i)** Quando uma pessoa executa uma série de assinaturas durante um período único e cotínuo de acesso controlado ao sistema, a primeira assinatura deve ser feita usando todos os componentes da assinatura; as assinaturas subseqüentes devem ser feitas usando pelo menos um componente eletrônico da assinatura, que seja executável por apenas uma pessoa e projetado para ser usado somente por ela. **(ii)** Quando a pessoa executa uma ou mais assinaturas que não são realizadas durante um período único e contínuo de acesso controlado ao sistema, cada assinatura deve ser feita usando todos os componentes eletrônicos da assinatura.	Requer reinserção do ID e senha do usuário durante a assinatura. Ambos componentes são solicitados em todas as assinaturas.
(2) Ser usada apenas por seus proprietários genuínos.	Os usuários podem somente alterar suas próprias senhas e nenhum acesso à leitura da senha é oferecido. Também é possível que os logins se encerrem após um período de inatividade configurado; limitar o número de tentativas de login antes de uma conta ser desabilitada; configurar um número mínimo de caracteres para senhas; e forçar o vencimento da senha após certo número de dias configurado, evitar o reuso da senha e forçar o uso de caracteres não-alfabéticos. O Data Reviewer Eurotherm também pode utilizar o Active Directory da Microsoft para gerenciar a autenticação do usuário.
(3) Ser administrada e executada para garantir que a tentativa de uso da assinatura eletrônica de um indivíduo por qualquer pessoa que não seja seu proprietário genuíno exija a colaboração de dois ou mais indivíduos.	Os usuários podem somente alterar suas próprias senhas e nenhum acesso à leitura da senha é oferecido. A menos que um usuário tenha compartilhado sua senha, uma auditoria completa será deixada. Com a opção de Audit Trail ativada, é ainda possível forçar as alterações pelo administrador do sistema para que as contas de usuário sejam autorizadas por um segundo indivíduo.

11.300 Controles de identificação de códigos / senhas	
As pessoas que utilizam assinaturas eletrônicas baseadas no uso de códigos de identificação combinados com senhas devem empregar controles que assegurem sua segurança e integridade. Tais controles devem incluir:	
(a) Mantendo a exclusividade de cada combinação entre código de identificação e senha, de modo que duas pessoas não tenham a mesma combinação de código de identificação e senha.	As contas de usuário são aposentadas. Todos os nomes de usuários são forçados a serem únicos.
(b) Assegurando que as emissões de código de identificação e senha são periodicamente verificadas, recuperadas ou revisadas (ex. para cobrir eventos como envelhecimento de senha).	É possível forçar uma senha para expirar após um número de dias configurado. Se um usuário deixa a empresa, sua conta pode ser marcada como aposentada.
(c) Seguindo os procedimentos de gerenciamento de perda para desautorizar eletronicamente tokens, cartões e outros dispositivos perdidos, roubados, ausentes ou potencialmente comprometidos que carregam ou geram informações de código de identificação ou senha e para emitir substituições temporárias ou permanentes usando controles rigorosos e adequados.	De acordo com Procedimento. Contas comprometidas podem ser desabilitadas. Na perda da senha, o administrador deve configurar uma nova senha para uma conta cujo detentor deve então substituir imediatamente por uma senha própria.
(d) Uso de proteções de transação para evitar uso não autorizado de senhas e/ou códigos de identificação e para detectar e informar de forma imediata e urgente para a unidade de segurança do sistema quaisquer tentativas de uso não autorizado e, quando apropriado, para o gerenciamento organizacional.	É possível que os logins se encerrem após um período de inatividade; limitar o número de tentativas de login antes de uma conta ser desabilitada; configurar um número mínimo de caracteres para senhas; e forçar o vencimento da senha após certo número de dias. Logins que falharam e desabilitaram contas são detalhados no *Audit Trail* no Data Reviewer Eurotherm.

Life Is On | Schneider Electric

Eurotherm Ltda

Av. Selma Parada, 201
Campinas SP
CEP: 13091-904
Brasil

Tel: +55 19 3112 5333

Email: vendas.eurotherm.br@se.com

www.eurotherm.com

Número do Documento HA033530BRA - Edição 1 SE Número do Documento 998-20998867-LMA_BR

Publicado em abril de 2020