REAL GRANDEZA
FUNDAÇÃO DE PREVIDÊNCIA E ASSISTÊNCIA SOCIAL

Ao acessar o Sistema Benner pela primeira vez, o Usuário concorda com a Política de Administração de Contas de Usuários, com os Termos e Condições de Uso do Sistema Benner, e com os requisitos do Termo de Confidencialidade, aqui disponíveis.

POLÍTICA DE ADMINISTRAÇÃO DE CONTAS DE ACESSO POR USUÁRIOS

DATA: 01/05/2015
VERSÃO: 1.0

Contexto
A Fundação Real Grandeza passou a gerir planos de saúde de beneficiários de distintas entidades. Para tanto, mantém equipe interna e fornecedores especializados, os quais necessitarão acessar as contas dos beneficiários, inclusive de forma remota.

Tendo em vista que tais contas contêm dados e informações pessoais, bem como os serviços e sistemas são de elevada importância para a adequada gestão, torna-se essencial controlar, dentre outros aspectos: (i) quem está acessando as informações ("usuário"); (ii) quando as informações são acessadas; e (iii) de onde é feito tal acesso. Tais controles pressupõem que cada usuário seja devidamente identificado e que tenha funções e privilégios claramente definidos.

O ciclo de vida do acesso por cada usuário será devidamente monitorado, garantindo a adequação a e a implementação das Políticas aplicáveis.

Objetivo e escopo
O objetivo desta Política é de definir procedimentos e controles de acesso ao Sistema Benner, e de prestação e/ou utilização dos Serviços de Gestão de Planos de Saúde, visando a proteção da privacidade, segurança e confidencialidade de todos os sistemas, recursos, aplicações e dados que componham e/ou integrem o Sistema Benner e os Serviços de Gestão de Planos de Saúde.

Esta Política aplica-se a todos os responsáveis pela criação, atribuição, extinção e administração de modo geral das contas de Usuário e/ou contas de acesso ao Sistema Benner e/ou a qualquer sistema compartilhado dos Serviços de Gestão de Planos de Saúde.

A Fundação manterá repositório central das identidades e informações de contas.

As Políticas de Segurança da Informação, Uso de Recursos Computacionais, bem como os Acordos de Confidencialidade se aplicam aos Administradores e Usuários de Contas de Acesso.

Definições
Acesso: capacidade de usar, modificar e manipular os dados e/ou as informações constantes do Sistema Benner e/ou obter acesso a um local e/ou espaço físico.

Confidencialidade: proteção de dados/ informações sigilosos de forma que não ocorra divulgação dos mesmos para indivíduos, entidades e ou processo não-autorizados.

Controle de Acesso: procedimento para negar ou outorgar requisições específicas acerca da obtenção e/ou uso de dados/ informações, com o propósito de proteger contra acesso ou uso não-autorizados do Sistema Benner.

Disponibilidade: proteção do Sistema Benner, bem como de dados e/ou informações, de forma que os Usuários autorizados possam acessar o Sistema de maneira segura e oportuna.

Princípio das prerrogativas mínimas: as prerrogativas de acesso de qualquer Usuário devem ser limitadas aos recursos necessários para o estrito cumprimento de suas funções e/ou deveres.

Princípio da Separação das Funções: uma única pessoa não deve ser responsável por completar ou controlar uma tarefa, ou conjunto de tarefas, do princípio ao fim, de forma a impedir/ evitar abusos, fraudes e outros danos, quando possível.

Identificação
Identificação é o processo de atribuição de um identificador para cada Usuário, em diferentes níveis de acesso.

Características dos identificadores:

- Único: cada identificador deve ser associado com uma única pessoa e/ou entidade;
- Unicidade: cada indivíduo terá tão somente um único identificador;
- Não-reutilização: uma vez que um identificador seja atribuído a uma pessoa e/ou entidade, tal identificador será sempre associado a tal pessoa/entidade e em hipótese alguma poderá ser re-atribuído para identificar outra pessoa e/ou entidade.

Cada Usuário será responsável pelo envio da informação completa, correta e atual para criação de sua conta de acesso. Será também responsabilidade do próprio Usuário a atualização dos dados sempre que necessário.

[PERIODICIDADE] os Administradores de Conta e/ou o próprio sistema realizarão uma varredura para identificar as Contas de Usuários inativas há ..... dias para que sejam tomadas as medidas cabíveis (incluindo a confirmação ou desativação da Conta de Usuário).

Autenticação
Autenticação é o processo empregado para confirmar que a pessoa e/ou entidade é efetivamente quem a pessoa e/ou entidade diz ser, validando a identidade da pessoa e/ou entidade. Os processos de autenticação incluem um identificador público (como nome de Usuário ou número de identificação) e informação de autenticação privada (como uma senha e/ou um número de identificação pessoal (PIN)).

O Sistema Benner e demais aplicações relacionadas à prestação de serviços de Gestão de Plano de Saúde utilizarão mecanismos de autenticação com criptografia, aderindo aos seguintes procedimentos:

- Credenciais de autenticação não podem ser inseridas (gravadas) em códigos de programas, exceto se não houver outra opção disponível;
- Senhas únicas serão inicialmente providenciadas por meio de método seguro e confidencial e serão alteradas pelo Usuário no primeiro acesso;
- Senhas não podem ser salvas em formato de texto ou em outro formato facilmente conversível;
- Senhas padrão programadas de fábrica ou senhas em branco serão imediatamente identificadas e alteradas no momento da instalação do Sistema Benner, programas e/ou aplicações relacionadas.

Como garantia de que as senhas possuem a segurança adequada, as senhas de Usuários, do Sistema Benner e de dispositivos que acessem remotamente o Sistema Benner devem atender aos seguintes requisitos mínimos de segurança, quando tecnicamente possível:

Requisitos da Senha	
Alteração da Senha	A cada 6 meses
Número mínimo de caracteres	8
Complexidade da Senha	Média
Histórico de senhas	
Bloqueio de conta	Após 4 tentativas consecutivas erradas
Tempo do bloqueio	
Renovação do pedido de log-in	Após 1 hora de inatividade do sistema
Protetor de Tela	Após 15 minutos, com proteção por senha

As contas de Usuários privilegiados (raiz, super usuário, e senhas de Administradores para servidores, bancos de dados, dispositivos de infra-estrutura e outros sistemas) tem que aderir aos parâmetros elencados acima e sempre que possível ao que segue:

- Autenticação para Usuários individualmente, e não em grupo;
    - Nos casos em que seja necessário para fins administrativos conta de grupo e senhas compartilhadas, tais senhas serão obrigatoriamente alteradas a cada 6 meses e imediatamente após a troca e/ou substituição de membro do grupo;
- Dispositivos configurados especialmente com separação para contas de Usuários privilegiados e contas de Usuários não-privilegiados;
- Dar preferência à autenticação de contas de Usuários não-privilegiados (ou seja, criar majoritariamente contas de Usuário não-privilegiados e excepcionalmente contas de Usuários privilegiados).

Autorização
Autorização é o procedimento empregado para dar permissão aos Usuários autenticados. Autorização concede ao Usuário, por meio de tecnologia ou processos, o direito de usar os ativos de informação e determina o tipo de acesso permitido (somente leitura, criar, apagar, e/ou modificar). O Sistema Benner ou aplicação de acesso deve determinar se o Usuário tem permissão para desempenhar a operação solicitada.

Os Usuários não terão permissão para acessar dados sigilosos, exceto nos casos em que o titular da informação tiver consentido por escrito por meio de um procedimento previamente estabelecido para esse fim.

Os Administradores devem garantir que todos os Usuários que tenham acesso à dados sensíveis participem de palestras e treinamentos adequados à sua proteção, bem como que conheçam e aceitem o Termo de Confidencialidade da Fundação.

Deveres de Segregação
Os privilégios de acesso concedidos a cada Usuário individualmente respeitarão o princípio da separação de deveres. Usuários técnicos e/ou administrativos, como programadores, Administradores de sistemas, de bancos de dados e /ou de segurança terão um acesso adicional e separado para quando utilizarem o Sistema Benner como Usuários finais.

Compliance
Os proprietários do Sistema documentarão os procedimentos de controle de acesso e apresentarão tal documentação sempre que necessário para fins de auditoria. Indícios de aprovação de conta, encerramento e desativação devem ser apresentados quando solicitados para fins de auditoria.

Deveres e Responsabilidades dos Administradores de Contas
Os Administradores de Contas:
serão indicados entre os ocupantes dos cargos de analista de saúde, dentro da Fundação;
gerenciarão as contas de acesso de maneira a mitigar riscos aos dados pessoais e à Fundação, protegendo a integridade do Sistema Benner, dos banco de dados e da informação armazenada;
garantirão a real necessidade de criação da Conta de acesso / Usuário;
deverão, ainda, monitorar a adesão à esta Política e garantir a implementação de medidas para prevenir ou remediar qualquer deficiência.