WWF
Política Interna

WWF INTERNACIONAL

Política de Informação e Segurança de Dados Pessoais

Data da Versão: 1 Julho 2018, actualizada da versão anterior de 4 Novembro 2013

1. Escopo e Propósito

Essa política estabelece a responsabilidade de todos os funcionários (em período integral ou parcial, remunerados ou não, temporários ou permanentes), estagiários, usuários corporativos, prestadores de serviços, consultores, contratados e agentes - que têm acesso ao WWF International (WWF), armazenadas eletronicamente ou não, processadas por ou em nome do WWF.

Esta política fornece a estrutura do WWF para segurança da informação, incluindo a segurança de dados pessoais, conforme definido neste documento. É a principal política sob a qual outras políticas relacionadas à segurança da informação residem.

O WWF está comprometido com todos os aspectos da proteção de dados pessoais e leva a sério seus deveres e deveres legais de seus funcionários e outros Usuários (definidos aqui), sob o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), o *Swiss Federal Data Protection Act* e outra legislação aplicável.

2. Definições

Segurança de Informação é o conjunto de processos pelos quais o WWF garante a confidencialidade, integridade e disponibilidade de suas informações comerciais críticas e confidenciais: o WWF protege contra divulgação a usuários não autorizados (confidencialidade), protege contra modificação de informações (integridade) imprópria e oferece suporte a acesso oportuno e confiável a informação (disponibilidade).

Dado Pessoal é qualquer informação relativa a uma pessoa singular identificada ou identificável; uma pessoa singular identificável é aquela que pode ser identificada, directa ou indirectamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador on-line ou a um ou mais factores específicos do ponto de vista físico, genético ou genético. identidade econômica, cultural ou social dessa pessoa natural, por exemplo, detalhes de contato, família (incluindo parentes e contatos de emergência), educação, histórico de emprego e status profissional, remuneração, desempenho no trabalho, detalhes de e-mail, internet e sistema de computador uso, detalhes da conta bancária, estado civil, detalhes da previdência social, etc. Categorias especiais de dados pessoais referem-se a dados pessoais que podem revelar assuntos delicados como (mas não limitado a) origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, dados genéticos, dados biométricos processados com o propósito de identificar unicamente uma pessoa natural, saúde ou vida sexual ou orientação. Dados pessoais e categorias especiais de dados pessoais são protegidos por legislação na maioria dos locais**.**

Assunto do Dado é um indivíduo cujos dados o WWF International processa.

Processamento de Dados é qualquer operação realizada em dados pessoais, seja ou não por meios automatizados, como coleta, registro, análise, armazenamento, alteração, recuperação, consulta, uso e divulgação.

Utilizadores de Dados (Utilizadores): todas as partes que têm acesso às informações do WWF International, incluindo funcionários (em período integral ou parcial, remunerados ou não, temporários ou permanentes), estagiários, usuários de negócios, provedores de serviços, consultores, contratados e agentes.

3. Política

- **Todos os dados** devem ser processados em conformidade com as leis aplicáveis e obrigações contratuais, e protegidos contra o processamento não autorizado ou ilegal, perda ou destruição acidental, ou danos.

- **Recursos de informação**, por exemplo, armazenamentos de dados, bancos de dados, arquivos compartilhados e dispositivos de computação (telefones, computadores, laptops, unidade flash USB), devem ser designados proprietários e identificados e inventariados pelo menos uma vez por ano e protegidos contra acesso não autorizado, uso indevido ou corrupção.

- **Os perímetros de segurança física** devem ser definidos e usados para proteger áreas que contêm informações altamente confidenciais (definidas aqui), incluindo recursos de processamento de informações. O equipamento deve ser mantido e **protegido** contra ameaças, falhas de energia, interferência ou dano.

- **O acesso** a dados e sistemas de informação só deve ser concedido com base na necessidade de conhecimento e atender aos termos da função de trabalho do funcionário. A alocação e o uso de direitos de acesso privilegiado devem ser restritos, controlados e monitorados.

- **Retenção**: Os dados pessoais não serão mantidos por mais tempo do que os propósitos para os quais foram coletados ou são exigidos por lei ou regulamentos.

- **Integridade de dados**. Os usuários que processam dados pessoais devem garantir que os dados sejam mantidos precisos, completos e atualizados, e os dados incorretos ou incompletos, tendo em vista o objetivo de sua coleta, são corrigidos ou destruídos.

- **Violação de dados** Todos os Usuários são obrigados a relatar imediatamente uma perda suspeita ou real, roubo ou dano a dados ou ativos de informação, conforme os protocolos de violação de dados do WWF, conforme comunicados de tempos em tempos. Os usuários devem seguir as instruções de gerenciamento para reduzir a perda e, se necessário, relatar a perda para as autoridades. Uma violação de dados ocorre quando há um acesso ou uso suspeito, ameaçado ou real por uma pessoa não autorizada, incluindo perda ou roubo; amansar; vírus, *worms, malware* em dispositivos; e-mails mal direcionados; senhas, códigos de segurança perdidos, roubados ou divulgados; perda de chave (s); ou divulgação de informações altamente confidenciais e confidenciais a pessoas não autorizadas. A denúncia de violações é um requisito legal para dados pessoais!

- **Declaração de Privacidade**: A Declaração de Privacidade Internacional do WWF (a “Declaração de Privacidade”) deve ser fornecida aos indivíduos no ponto em que obtemos dados pessoais de um indivíduo (por exemplo, engajamento on-line, correspondência por e-mail, contratação de consultoria).

- **Processamento justo de dados pessoais**. O processamento de dados pessoais deve ser consistente com a Declaração de Privacidade. Os dados pessoais devem ser processados somente para o propósito pretendido. Dados pessoais obtidos para uma finalidade não podem ser usados para um propósito novo e não relacionado. O processamento deve ser justificado por uma de várias condições para processamento, como:

    - O indivíduo deu seu consentimento para o processamento.
    - O processamento é necessário para entrar ou executar um contrato com o titular dos dados.
    - O processamento é necessário para o cumprimento de qualquer obrigação legal a que o WWF Internacional esteja sujeito.

O processamento de categorias especiais de dados pessoais só deve ser feito quando for absolutamente necessário fazê-lo, e os direitos de acesso devem ser estritamente limitados. Uma das seguintes condições deve ser satisfeita para processar este tipo de dados:

- O consentimento explícito do indivíduo foi obtido;
- O processamento é necessário para uma obrigação nos termos da lei;
- Os interesses vitais do indivíduo precisam ser protegidos (por exemplo, em uma emergência médica ou outro cenário de vida ou morte);
- O processamento é necessário para fins de processos judiciais ou assessoria jurídica o no contexto do monitoramento da igualdade de oportunidades.

- **Avalie o impacto da privacidade**. Para uma atividade que utiliza dados pessoais (por exemplo, campanha on-line), os Usuários devem considerar se uma avaliação de impacto de privacidade (PIA) deve ser concluída para destacar e abordar os riscos para os dados pessoais a serem coletados. Orientação está disponível na realização de PIAs do Conselho Geral ou Conformidade.

4. Dados Seguros Por Classificação

Os usuários devem tomar medidas de segurança técnicas e organizacionais apropriadas para impedir o uso, divulgação, acesso, destruição, alteração ou danos não autorizados ou ilegais aos dados. Os usuários que têm acesso a dados pessoais estão sob a responsabilidade legal de tratá-los como altamente confidenciais. Os usuários devem entender o nível de confidencialidade dos dados e lidar com eles de acordo com as medidas de segurança apropriadas, conforme descrito abaixo.:

Classificação	Descrição	Medidas de Segurança	Exemplos
Dados Altamente Confidenciais	Informações que estão sujeitas ao mais alto nível de proteção, pois o acesso e o processamento não autorizados podem causar sérios danos aos indivíduos (por exemplo, roubo de identidade) e criam riscos legais e de reputação para a organização. **TODOS OS DADOS PESSOAIS SÃO ALTAMENTE CONFIDENCIAIS!**	Acessado apenas por pessoas autorizadas em uma base estritamente necessária para o conhecimento. Proteger com senha. Mantenha registros em papel em armários trancados Os processos de armazenamento, armazenamento, processamento e transferência são documentados e compreendidos pelos usuários relevantes. Os dados são armazenados com a mais alta segurança (escritório trancado; sistemas protegidos com acesso limitado, etc). Evite a transferência de e-mail e, se usado, proteja com senha. A violação desses dados deve ser imediatamente comunicada à gerência sênior	*Dados pessoais* de funcionários, doadores, consultores, apoiantes, etc. (salário e benefícios, procedimentos disciplinares, dados médicos etc.); detalhes do passaporte, data de nascimento, cartão de crédito ou números de contas bancárias; perfil de riqueza, etc.
Informação Condifencial	Informações (além de dados pessoais), que são críticas para os negócios e prejudicariam o WWF se publicadas em domínio público ou protegidas por regulamentos, políticas internas ou obrigações contratuais.	Acessado apenas por pessoas autorizadas em uma base de necessidade de conhecimento. Armazene em locais seguros. Transferência via e-mail ou outro é marcado como "confidencial / não para distribuição" ou protegido por senha. Mantenha registros em papel confidenciais e altamente confidenciais em gabinetes trancados.	Contrato de parceiro ou serviço com cláusula de confidencialidade. E-mails internos, memorandos e rascunhos não destinados a, ou antes de, lançamento público Lista telefônica interna
Informação Pública	Informações disponíveis ao	Antes da publicação, as informações são verificadas	Informações sobre sites públicos da WWF

Classificação	Descrição	Medidas de Segurança	Exemplos
	público, cuja divulgação não causaria danos a indivíduos, operações ou reputação da WWF.	pelo gerenciamento quanto à precisão e qualidade. Somente funcionários autorizados podem publicar ou comunicar publicamente.	Informações disponíveis publicamente sobre administradores e administradores

Em todo caso, *NÃO O FAÇA….*

- Postar informações não públicas em um site público.
- Compartilhar ou discutir informações não públicas com terceiros ou com aqueles do WWF que não têm necessidade de conhecer o negócio.
- Remover informações altamente confidenciais e confidenciais na forma física dos escritórios.
- Deixar informações confidenciais ou altamente confidenciais sem supervisão (por exemplo, em uma impressora).
- Tente obter acesso a sistemas e aplicativos se você não tiver credenciais apropriadas.

E Em Todos os Casos, Faça…

- Respeite a política de limpeza da mesa
- Consulte as diretrizes de média social do WWF International se estiver se comunicando através das Mídias sociais.
- Respeite a confidencialidade das informações em todos os momentos, mesmo depois de sair do WWF.

5. Senhas

Todos os sistemas e aplicativos devem ser protegidos por senha. As senhas devem:

- Atender aos requisitos de comprimento e complexidade;
- NUNCA ser compartilhado (exceto com o administrador do sistema para executar o suporte técnico e, posteriormente, deve ser imediatamente alterado);
- Ser alterado se forem senhas temporárias ou padrão atribuídas pelo fornecedor ou ICT;
- NUNCA seja escrito em um local acessível;
- DEVE ser diferente para diferentes sistemas para mitigar o risco em caso de violação de segurança; e
- NUNCA seja salvo, especialmente em computadores não-WWF ou públicos.

Por favor, consulte a Política de Senha para mais detalhes

6. Uso inteligente de ativos de informação

Uso de dispositivos / hardware de computador

Os usuários devem tomar medidas para evitar o acesso não autorizado ou a perda de dados ou o roubo de dispositivos de computação: computadores de mesa, laptops, *smartphones, tablets*, discos flash, unidades externas, etc...

- Informações altamente confidenciais devem primeiro ser criptografadas (consulte as diretrizes de criptografia aqui) se armazenadas em computadores e dispositivos de armazenamento (como discos portáteis, discos rígidos externos, unidades flash, CDs e DVDs).

- Sempre senha / código proteger seus dispositivos e configurá-lo para bloqueio automático após 5 minutos de inatividade.
- Os dispositivos de computação devem estar devidamente protegidos (por exemplo, bloqueados ou bloqueados em gabinetes, se não estiverem em uso).
- NÃO danifique, altere ou use indevidamente qualquer hardware de propriedade ou mantido pelo WWF.
- Sempre desconecte ou bloqueie a tela quando deixar seu computador sem supervisão.
- NÃO deixe dispositivos móveis desacompanhados.
- Ao usar computadores públicos (a) nunca salve suas senhas, (b) exclua todas as informações salvas, (c) feche todas as sessões e (d) limpe todos os dados armazenados em cache e exclua todos os arquivos temporários.
- NÃO utilize software ou dispositivos não autorizados (por exemplo, computador doméstico) para processar informações altamente confidenciais e confidenciais.
- Ao baixar aplicativos, verifique se o acesso deles aos recursos do dispositivo, como contatos, calendário, e-mail, etc., está de acordo com esta política.

Uso de Dispositivos Pessoais

Como regra geral, somente dispositivos WWF têm permissão para acessar os sistemas WWF, e-mail, calendários, contatos, documentos, etc., e o uso de dispositivos pessoais não é permitido. No entanto, o uso incidental de dispositivos pessoais é permitido, sujeito aos seguintes:

- o uso deve ser especificamente autorizado pelo gerente direto do funcionário;
- o dispositivo pessoal deve ser configurado por ICT, ser protegido por senha e atualizado com as mais recentes proteções e atualizações antivírus (incluindo aplicativos de segurança exigidos pela ICT);
- os dados pessoais devem ser claramente separados dos dados do WWF;
- após cada sessão, todos os aplicativos ou serviços relacionados a negócios devem ser desconectados;
- os usuários devem cumprir as políticas do WWF, todas as leis aplicáveis e as instruções do fabricante, e os usuários podem ter responsabilidade pessoal por qualquer uso indevido do dispositivo pessoal;
- qualquer gravação de áudio ou vídeo deve ser especificamente autorizada.
- antes de viajar para o exterior, os usuários devem entrar em contato com a TIC para determinar se as restrições locais se aplicam em relação ao dispositivo ou software;
- adicionalmente, para dados altamente confidenciais e / ou confidenciais - somente acesso sem fio seguro deve ser usado para trocar esses dados; exceto se o dispositivo estiver protegido por criptografia, esses dados devem ser excluídos imediatamente após o uso ou quando não forem mais necessários (incluindo todos os dados armazenados nos arquivos temporários).

- O direito de usar dispositivos pessoais é um privilégio e pode ser revogado se usado incorretamente. Além disso, o WWF tem o direito de limpar o dispositivo (por exemplo, para garantir a segurança de determinados dados em caso de perda ou roubo do dispositivo pessoal e rescisão de contrato de trabalho), ou para solicitar a entrega do dispositivo pessoal, em cada caso para o medida permitida por lei.

Evitando hacks, malware, etc.

- Nunca abra anexos de e-mail suspeitos, responda a spam de phishing ou navegue para sites não confiáveis.
- Nunca baixe documentos da Internet, a menos que sejam selecionados com software antivírus antes do uso.

Trabalhando na rede, na Internet e na nuvem

- O acesso remoto a informações confidenciais só é permitido através de rede segura e dispositivos autorizados pelo WWF.
- A transferência de informações altamente confidenciais e confidenciais deve ser protegida com métodos apropriados (por exemplo, aplicação segura de transferência de arquivos, criptografia, VPN, etc.).
- Os usuários devem evitar visitar sites não confiáveis.
- Os dados coletados na Internet devem ser verificados e confirmados antes de serem usados quanto à precisão e também para quaisquer direitos de propriedade intelectual que possam ser aplicados.
- Sempre opte por uma conexão segura com a Internet e assegure-se de que o dispositivo que você está usando esteja atualizado com a proteção contra vírus; e depois de ter terminado sua sessão, que você faça o logout completamente e exclua todos os dados em cache (incluindo aqueles nos arquivos temporários). Se estiver usando um computador público, aplique as mesmas regras conforme indicado aqui.

7. Construindo Segurança de Acesso

Aqueles que utilizam as instalações do WWF devem respeitar os procedimentos de segurança de acesso ao edifício.

8. Descarte de Informações Confidenciais / Altamente Confidenciais

O descarte de informações confidenciais e altamente confidenciais deve garantir que elas não possam ser recuperadas ou reconstituídas. Registros em papel devem ser redigidos ou fragmentados e nunca devem ser descartados no todo**. Computadores, laptops, discos rígidos de impressora** e outros dispositivos de armazenamento eletrônico devem ser totalmente excluídos (usando software apropriado ou destruindo fisicamente) e entregues a TIC.

9. Empreiteiros e outros fornecedores

Todos os fornecedores que coletam, processam, armazenam ou têm acesso a informações confidenciais ou confidenciais do WWF devem ter um contrato por escrito aprovado pelo Conselho Geral Internacional do WWF, que cobre a prestação de serviços e impõe todas as obrigações do usuário nesta política. A TIC tem o direito de realizar uma auditoria de segurança dos sistemas e processos do fornecedor.

10. Solicitações de acesso a dados

Nunca divulgue informações para as quais o WWF tenha um contrato de confidencialidade com outra parte proibindo ou restringindo tal divulgação. Um funcionário que recebe uma solicitação, seja de organizações externas ou indivíduos, para acessar dado confidencial ou altamente confidencial deve agir de acordo com essa política e, em caso de dúvida, deve entrar em contato com o Conselho Geral. Os usuários são

obrigados a cooperar com o Conselho Geral ou com a alta administração na resposta a solicitações de acesso de indivíduos. No entanto, os titulares dos dados têm o direito de aceder aos seus dados pessoais mediante pedido e de os alterar, corrigir ou eliminar de acordo com a nossa Declaração de Privacidade. Os titulares dos dados podem contatar o WWF em supportercare@wwfint.org para solicitar qualquer um dos itens acima..

11. Responsabilidades

A gerência deve garantir que essa política seja compreendida por todos os usuários. O WWF irá monitorar, realizar auditorias e tomar outras medidas para garantir a conformidade com esta política.

Equipe de departamento de TIC e Administradores de Sistemas: dão suporte ao Gerenciamento para aplicar esta política no que se refere à proteção de sistemas, hardware e software de TIC.

O não cumprimento desta política pode levar a medidas disciplinares, incluindo até demissão sumária. Se você for consultor, contratado ou fornecedor, o não cumprimento desta política constituirá quebra de contrato e resultará na rescisão imediata de seu contrato com a WWF. Além disso, tais violações podem levar a ação criminal e / ou civil iniciada contra você. Os direitos de acesso dos usuários podem ser restringidos ou suspensos durante as investigações. Quaisquer dúvidas sobre esta Política devem ser levantadas com o seu gerente ou com o seu Conselheiro Geral.

O WWF revisará esta política de tempos em tempos e a atualizará para cumprir as mudanças na legislação e em sua organização e procedimentos internos. Quaisquer versões atualizadas desta política serão comunicadas a todos os usuários por escrito em tempo hábil**.**

12. Outras Políticas Relacionadas

A WWF criará, de tempos em tempos, novas políticas ou atualizará as existentes, o que detalhará ainda mais os requisitos mencionados acima. Aqui está uma lista de políticas actuais:

- Proteção de Dados do Funcionário
- Declaração de privacidade
- Protocolo de Violação para Funcionários
- Política de mesa limpa
- Política de senha
- Uso de email
- Criptografando informações confidenciais

Esta Política foi aprovada por:

Linda Humphrey	Dominic O'Neill
Director ICT	Exec. Director, Operations