Lisbon School of Economics & Management
Universidade de Lisboa

REGULAMENTO INTERNO

(RG-PRE-01/V02)

INDICE

1. Código de conduta

1.1 Respeitar as políticas internas e leis aplicáveis

Os Colaboradores do **ISEG** devem agir sempre em conformidade com as políticas e processos internos e as leis vigentes em Portugal e na Comunidade Europeia.

A manutenção da reputação do **ISEG** depende das atitudes individuais integras de cada Colaborador que representam a imagem da organização.

1.2 Valorizar a responsabilidade pessoal

O **ISEG** atribui grande valor aos seus Colaboradores, promovendo uma relação de confiança, respeito e reconhecimento da contribuição individual de cada um. Procura estabelecer e manter um bom ambiente de trabalho em equipa, desafio e desenvolvimento pessoal e uma comunicação clara, aberta e construtiva.

1-3 Respeitar a diversidade

Mostramos um comportamento que se carateriza pela aceitação e pela tolerância.

Desaprovamos qualquer relacionamento que se carateriza por violência verbal ou física, por insultos ou pela vergonha.

Ao respeitarmos diferentes culturas, não toleraremos qualquer discriminação, assédio ou retaliação contra qualquer indivíduo ou grupo com base em fatores étnicos, sexuais, raciais, religiosos ou culturais, nem qualquer outra característica protegida pela lei vigente.

Visamos igualdade de oportunidades a todos Colaboradores de acordo com o seu mérito, aptidões, qualificações, experiência, esforço e capacidade de desempenhar as suas funções.

1.4 Trabalhar em ambiente livre de assédio

O **ISEG** está empenhado em oferecer um ambiente de trabalho no qual não é tolerada qualquer forma de assédio moral e sexual. O assédio é um comportamento indesejado (gesto, palavra, atitude) nomeadamente baseado nalgum fator discriminatório (por ex. sexo, nacionalidade, deficiência etc.) e praticado com algum grau de repetição com o objetivo ou o efeito de afetar a dignidade da pessoa ou criar um ambiente intimidativo, hostil, degradante, humilhante ou desestabilizador.

1.5 Proteger a privacidade

O **ISEG** assume o compromisso de respeito dos requisitos do Regulamento Proteção de Dados Pessoais - Regulamento (UE) 2016/679 RGPD ou GDPR de 27 de abril de 2016, a retificação de 23.5.2018 e a Lei nº 58/2019 relativos à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados de acordo com a Política de Privacidade publicada e em vigor.

O Colaborador assume um compromisso de confidencialidade e sigilo da informação do **ISEG**, dos seus Alunos e outros titulares, durante e após o termo do Contrato de trabalho e na receção do atual regulamento interno.

Todos os Colaboradores devem conhecer e cumprir os princípios de privacidade no tratamento dos dados pessoais que tenham acesso no desempenho das suas funções.

Sempre que um colaborador detetar um potencial incidente de segurança e privacidade, deve comunicá-lo diretamente ao Encarregado de Proteção de Dados EPD / DPO Dr. Tiago Abade (Email: rgpd@ulisboa.pt.).

1.6 Trabalhar em segurança

Todos os Colaboradores devem conhecer e cumprir os requisitos e legislação aplicável à saúde e segurança no trabalho.
O **ISEG** recorre a uma organização subcontratada especializada para a prestação de serviços de Medicina no Trabalho e manutenção das condições de higiene e segurança das instalações.

1.7 Preservar o meio ambiente

Proteger o meio ambiente é uma prioridade para a **ISEG** que se compromete a cumprir com as leis e regulamentos ambientais vigentes. Consequentemente, esperamos que os Colaboradores: manuseiem, armazenem e eliminem corretamente os resíduos; cumpram as autorizações ambientais aplicáveis; e informem a Presidência e Administrador relativamente a qualquer violação real ou potencial da regulamentação ambiental aplicável.

2. Regras de Conduta

2.1 Direitos de autor e propriedade intelectual

1. Todos os colaboradores são responsáveis por cumprir com os requisitos das licenças de software relacionados com os pacotes de software usados no cumprimento das suas responsabilidades profissionais.
2. A lei dos direitos de autor não permite a cópia ou a distribuição de software e o não cumprimento desta lei pode levar a organização e até o próprio Colaborador a incorrer em penalidades no âmbito de processos disciplinares.
3. O controlo da instalação de software licenciado é da responsabilidade da Direção de Informática do **ISEG**.

2.2 Classificação da informação

O **ISEG** considera a seguinte Política de classificação da informação:

Informação Pública: A informação que não contenha conteúdo sensível nem quaisquer dados pessoais de titulares que não deram o seu consentimento a ser disponibilizada a entidades externas, sejam eles parceiros, Alunos e ou entidades públicas. Trata-se normalmente de informação publicada na página internet.

Informação Interna: Informação da organização que pelo seu nível de baixa sensibilidade e valor e alta necessidade de acessibilidade, deve ser do conhecimento dos Colaboradores Docentes e Não Docentes do **ISEG** e não deve ser transmitida a elementos externos da organização. Trata-se normalmente de documentos do Sistema de Gestão Integrado como Políticas, processos, modelos, regras organizacionais, comunicações internas institucionais.

Informação Confidencial: Informação da organização, dos Alunos, dos candidatos, dos ex alunos, dos restantes colegas, dos fornecedores e **dados pessoais** dos seus titulares que pelo seu nível de alta sensibilidade e valor e baixa necessidade de acessibilidade deve ser apenas do conhecimento de um número restrito de Colaboradores Docentes e Não Docentes e/ou outras pessoas nomeadas. São confidenciais os dados pessoais sensíveis como dados de saúde e necessidades especiais.

2.3 Manipulação de informação confidencial

1. A informação confidencial deverá residir na rede do **ISEG** protegida por acessos restritos autenticados e não deverá estar armazenada no disco local do computador de cada colaborador
2. A informação confidencial que se encontre armazenada em dispositivos móveis (PC's, Pen's, Discos Externos), deverá sempre que possível protegida contra furto ou acessos não autorizados através de encriptação
3. A transmissão de informação confidencial digital (por exemplo por email) tem de ter protegida com palavra passe
4. Não devem ser utilizados serviços públicos gratuitos de partilha de ficheiros (google drive, dropbox) para transferência ou arquivo de informação confidencial
5. A impressão de informação confidencial deverá ser protegida contra acesso não autorizado, em armário fechado e/ou sala de acesso restrito
6. A informação confidencial não deverá ser comentada em locais públicos (restaurantes ou transportes públicos).

2.4 Uso aceitável dos ativos do ISEG

1. Os sistemas de informação do **ISEG** devem ser utilizados como meio de auxílio às atividades, sendo a sua utilização passível de ser auditada / monitorizada através de auditorias aos equipamentos e/ou análise de logs de acesso tendo em vista a manutenção dos equipamentos e dos níveis de segurança e conformidade às regras internas, leis e regulamentação aplicáveis
2. A instalação de software nos sistemas de informação do **ISEG** só poderá ser realizada com o conhecimento da Direção de Informática para garantia do cumprimento de licenciamento
3. O uso, para fins pessoais, de equipamento ou recursos que são pertença do **ISEG** terá de ser autorizado pela Direção de Informática e deve ser identificada como "informação pessoal" em área de rede pessoal
4. Está restrita a utilização dos sistemas de informação do **ISEG** para o envio ou receção de material ofensivo ou discriminatório
5. Os colaboradores devem alertar para todas as situações que possam levar a dano, furto ou utilização indevida
6. No fim do dia ou em situação de ausência, o Colaborador deve arrumar o espaço de trabalho, protegendo os documentos e dispositivos com informação confidencial
7. Nas impressoras, corredores, salas de reuniões ou espaços comuns não deve ser deixada informação sem vigilância.

2.5 Acessos lógicos

1. A atribuição / atualização de acessos individuais (login / password) a cada colaborador é realizada pela Direção de Informática do **ISEG**, de acordo com o perfil funcional
2. As palavras-chave são pessoais e intransmissíveis e seguem o descrito na política de passwords
3. Não é permitido a um colaborador assumir indevidamente a identidade de outro nem autorizar que assumam a sua
4. Se um colaborador utilizar um dispositivo que possa estar a partilhar com outro colaborador, deve sempre iniciar a sua sessão (utilizador/palavra-chave)
5. Não é permitido utilização de *clouds* públicas ou sistemas de envio de ficheiros de grande dimensão (Ex: wetransfer)
6. Deverão ser ativados proteções de ecrãs com palavras-chave, sempre que o utilizador se ausentar
7. Deverá ser feito *logoff* às aplicações e sistemas sempre que não necessite de os utilizar
8. Todos os colaboradores que necessitem de se ligar aos sistemas e redes do **ISEG**, a partir de um ponto exterior (ex. teletrabalho), deverão possuir uma ligação segura (via VPN) autorizada pela Direção de Informática do **ISEG**

9. No fim de contrato os acessos do utilizador serão desativados e a informação pessoal eventualmente arquivada em rede será eliminada.

2.6 Acessos físicos

1. A atribuição / atualização de acessos individuais (cartão de identificação) a cada colaborador é realizada pelo DLAT tendo em vista a segurança das instalações e pessoas
2. No caso de perda do cartão, o Colaborador deve comunicar ao DLAT / Segurança
3. O colaborador que recebe um visitante deve zelar pelo seu conhecimento das regras de conduta de visitantes e garantir o seu encaminhamento dentro da organização

2.7 Uso da internet e correio eletrónico

1. O correio eletrónico (email) é um importante meio de comunicação oficial
2. Os emails enviados ou recebidos devem ser tratados consoante o nível de classificação da informação em causa
3. O serviço de email não é considerado totalmente seguro pois conteúdos do email passam por redes públicas e privadas
4. Para partilha de informação interna devem ser utilizadas áreas de rede acedidas entre as partes
5. O Colaborador é responsável pela atividade desenvolvida na sua conta e caixa de correio
6. Qualquer ficheiro externo introduzido na rede deve cumprir os requisitos de propriedade intelectual e controlo de vírus
7. Não deve divulgar listas de emails, logo, sempre que não seja estritamente necessário cada destinatário conhecer os restantes, deve optar pelo BCC (cópia oculta) em detrimento do CC (cópia com conhecimento)
8. Não é permitido difundir conteúdos ilegais, religiosos ou políticos
9. Não é permitido o envio de correio eletrónico a pessoas que não o desejam receber
10. Não é permitido efetuar ataques para obstruir sistemas informáticos ou qualquer atividade que tenha como objetivo a paralisação do serviço por saturação de linhas de comunicação, da capacidade de processamento do servidor, ou similar
11. Nunca abrir sites desconhecidos ou de origem duvidosa
12. Todos os programas de proveniência duvidosa não deverão ser executados.

2.8 Uso de redes sociais

1. **PESSOAIS** - O uso de redes sociais pelos Colaboradores poderá colocar em risco informações confidenciais e reputação do **ISEG**, pelo que nenhuma informação confidencial sobre o **ISEG**, Alunos, candidatos, colegas e/ou fornecedores, pode ser divulgada via redes sociais pessoais.
2. **ISEG** - Só pode ser difundida informação que seja aprovada pelo Marketing, respeitando a confidencialidade e os consentimentos expressos dos titulares dos dados envolvidos.

2.9 Política de cópias de segurança

O **ISEG** assegura a realização de cópias de segurança à informação constante nos servidores e aplicações, incluindo o correio eletrónico.

1. É da responsabilidade de cada colaborador salvaguardar ficheiros de trabalho nas áreas de arquivo da rede.
2. Não é realizada cópia de segurança à informação armazenada no disco local dos computadores.

2.10 Palavras passe

As palavras passe são pessoais e intransmissíveis. A escolha da palavra passe é do critério do utilizador, ficando este obrigado a cumprir com as seguintes normas de construção:

1. Deve ter sempre que possível mais de 7 posições de comprimento, letra maiúscula, letra minúscula, número e/ou carácter especial
2. Não deverá conter informação de índole pessoal, como por exemplo, nomes próprios, apelidos, número de telefone, datas de nascimento, matrículas de automóvel, etc.
3. Se receber uma palavra passe por defeito deve alterá-la na primeira utilização
4. A palavra passe não deverá ser apresentada no monitor quando estiver a ser inserida
5. A palavra passe não deverá ser escrita em local visível e facilmente acessível
6. A palavra passe poderá ser memorizada ou guardada em ficheiro com palavra passe / encriptado
7. Não utilizar a mesma palavra passe para acessos profissionais (rede, aplicações) e pessoais (redes sociais)
8. Não permitir ao browser/windows memorizar/registar a palavra passe
9. Alterar periodicamente a palavra passe e sempre que suspeitar ataque à segurança da informação.

2.11 Proteção contra vírus ou software malicioso

1. Os sistemas informáticos do **ISEG** deverão dispor de um software antivírus ativado automaticamente
2. Quaisquer programas ou software provenientes de fontes desconhecidas ou cuja proveniência é duvidosa não deverão ser executados e deverão ser eliminados de imediato
3. Sempre que se aceder a dados e/ou executar programas a partir de um disco/pen, os colaboradores deverão submetê-los à verificação pelo programa de antivírus antes de lhes acederem pela primeira vez
4. Sempre que um colaborador detetar no seu posto de trabalho comportamentos suspeitos de serem atacados por vírus deve contactar de imediato a Direção de Informática do **ISEG**.

2.12 Conflito de interesses

Um "conflito de interesses" ocorre quando os interesses pessoais do Colaborador interferem ou parecem interferir com os interesses do ISEG. Consequentemente, os Colaboradores não devem ter interesses diretos ou indiretos que possam potencialmente prejudicar a sua objetividade, independência de julgamento ou conduta no cumprimento das suas responsabilidades em nome do **ISEG**.

Os Colaboradores devem cumprir o plano de gestão de riscos de corrupção e infrações conexas do **ISEG** em vigor.

3. Privacidade de dados pessoais

3.1 Licitude, finalidade e preservação de dados pessoais do Colaborador

O **ISEG**, na qualidade de responsável pelo tratamento, para realização das atividades relacionadas com a gestão do contrato de trabalho procederá ao tratamento dos seguintes dados de carácter pessoal, nomeadamente:

a) Dados de identificação, fiscais, email pessoal e fotografia de identificação;
b) Situação familiar: estado civil, dados do agregado familiar para efeitos fiscais;
c) Atividade profissional: horário e local de trabalho, número de identificação interno, data de admissão, função, nível salarial, natureza do contrato, avaliação de desempenho;
d) Elementos relativos à retribuição: retribuição de base, outras prestações certas ou variáveis, subsídios, férias, assiduidade e absentismo, licenças, outros elementos relativos à atribuição de complementos de retribuição, montante ou taxa em relação aos descontos obrigatórios ou facultativos;
e) Outros dados: dados de saúde relativos à medicina no trabalho, doenças profissionais e acidentes de trabalho; dados de ações judiciais e penais, eventual grau de incapacidade respetivo ou de membro do seu agregado familiar, local e forma dos pagamentos a efetuar pelo Empregador, número de conta bancária e identificação da instituição.

O **ISEG** poderá comunicar e/ou transferir os dados pessoais dos Colaboradores às entidades seguintes, com vista às seguintes finalidades da gestão contratual e cumprimento da legislação aplicável:

a) IGFSS – Instituto de Gestão Financeira da Segurança Social
b) AT – Autoridade Tributária
c) Instituições Bancárias, Corretora de Seguros e Seguradora
d) ACT – Autoridade para as Condições do Trabalho
e) Empresa de Segurança, Higiene e Medicina no trabalho
f) Tribunais ou outras entidades judiciais equivalentes;
g) Entidades inspetoras e auditoras;

De acordo com Política de Retenção de Dados Pessoais, os dados pessoais serão destruídos logo que termine a sua licitude e finalidade, ou seja, fim da relação laboral e fim do período de preservação imposto pela lei aplicável.

3.2 Direitos do Colaborador

Como titular dos dados pessoais, tem os seguintes direitos que pode exercer via comunicação escrita junto da Direção de Recursos Humanos / Administrador:

a) Direito de obter a confirmação de que os dados que lhe digam respeito são ou não objeto de tratamento e, se for o caso, de aceder aos seus dados pessoais e aceder às informações previstas na lei
b) Direito a que o **ISEG**, sem demora injustificada, retifique os dados inexatos ou incompletos que lhe digam respeito
c) Direito de solicitar o apagamento dos seus dados, sem demora injustificada, quando os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento.
d) E ainda tem o direito de apresentar uma reclamação junto da Autoridade de Controlo ao abrigo do Regulamento Geral de Proteção de Dados Pessoais que em Portugal é a CNPD Comissão Nacional de Proteção dos Dados Pessoais.

3.3 Tratamento da imagem do Colaborador

O **ISEG**, salvaguarda a privacidade da imagem pessoal dos seus Colaboradores com as seguintes licitudes e finalidades:

a) **Contrato de trabalho** podendo a fotografia de identificação ser comunicada internamente e externamente (na página internet e rede social do **ISEG**, gravação de eventos institucionais, newsletter institucional) para efeitos de representação da função na Escola, segurança das pessoas e organização do serviço junto da Comunidade académica - aplicável aos Dirigentes e Colaboradores Docentes e Não Docentes nas funções de Coordenação
b) **Consentimento** específico, livre e expresso pelos Colaboradores Docentes e Não Docentes, nas restantes situações

3.4 Tratamento da imagem de Alunos

1. Os Alunos expressam o consentimento livre e específico relativamente ao tratamento da sua imagem pessoal em eventos institucionais, newsletter institucional ou outras
2. O consentimento específico é gerido pela área de Marketing

3.5 Tratamento de dados no âmbito da Pandemia COVID

1. **Controlo de temperatura corporal, se aplicável:**
   O Colaborador que realiza o controlo de temperatura está obrigado ao dever de confidencialidade e privacidade.
   São definidos procedimentos subsequentes à deteção de um caso de temperatura igual ou superior a 38ºC, que garantam e assegurem a discrição e a dignidade do tratamento da pessoa objeto do controlo.
2. **Realização de testes de diagnóstico de SARS-CoV-2:**
   Os testes de diagnóstico são realizados por um profissional de saúde, sujeito à obrigação de sigilo profissional.
   São definidos procedimentos subsequentes à deteção de um caso de resultado positivo, que garantam e assegurem a discrição e a dignidade do tratamento da pessoa objeto de testes.
3. **Reforço da capacidade de rastreio por quem não seja profissional de saúde:**
   O Colaborador mobilizado está vinculado expressamente, no ato jurídico que determine a mobilização ou em declaração jurídica autónoma, a um específico dever de confidencialidade e privacidade relativamente a todos os dados pessoais que venha a conhecer, no exercício destas funções.

3.6 Violação do Código de Conduta

As implicações disciplinares da violação do presente Regulamento Interno e Código de Conduta são as constantes da Lei Geral do Trabalho em Funções Públicas em vigor.

4. Aprovação

A aprovação do presente Regulamento Interno pressupõe o respeito pelo Código de Conduta e de Boas Práticas da Universidade de Lisboa em vigor.

Estas regras e orientações do Regulamento Interno foram aprovadas pela Presidência e revogam as orientações anteriores sobre os mesmos assuntos.

A Presidente

Doutora Clara Raposo

4.1 Histórico de versões

Versão	Data	Razão para a nova versão
01	03-02-2021	Versão inicial
02	02-03-2021	Alteração dos pontos: 2.5 Acessos lógicos 2.7 Uso da internet e correio eletrónico