Codi de Conducta de Seguretat de la Informació

Institut de Recerca Germans Trias i Pujol

APROVACIÓ

Responsable: CARLES ESQUERRÉ
Gerent IGTP

DATA: 09 d'octubre de 2019
Signat

INDEX

1. FINALITAT, ABAST I USUARIS 3
1.1. DEFINICIONS 3
2. CONFIDENCIALITAT I SEGURETAT DE DADES PERSONALS I INFORMACIÓ CONFIDENCIAL 3
2.1. DADES PERSONALS 3
2.2. INFORMACIÓ CONFIDENCIAL 4
2.3. MESURES DE SEGURETAT 4
2.3.1. Protegir informació confidencial o sensible 4
2.3.2. Dades Mèdiques 4
2.3.3. Destrucció d'arxius que continguin dades personals i/o informació confidencial 5
3. POLÍTICA DE TAULA I PANTALLA NETA 5
3.1. PROTECCIÓ AL LLOC DE TREBALL 5
3.1.1. Política de taula neta 5
3.1.2. Política de pantalla neta 5
3.1.3. Contrasenyes 5
3.2. PROTECCIÓ D'INSTAL·LACIONS I EQUIPAMENTS COMPARTITS 6
4. EQUIP INFORMÀTIC MÒBIL 6
4.1. INTRODUCCIÓ 6
4.2. NORMES BÀSIQUES 6
5. TELETREBALL 7
6. ÚS DE DISPOSITIUS PROPIS 7
6.1. NORMES PER GARANTIR LA SEGURETAT EN L'ÚS DE DISPOSITIUS PROPIS 7
6.1.1. Política de l'organització 7
7. COMENTARIS O PREGUNTES 7
8. REFERÈNCIES 8

1. Finalitat, Abast i Usuaris

El propòsit d'aquest document és definir normes per evitar l'accés no autoritzat a:

- Informació als llocs de treball, així com a equipaments i espais compartits.
- Dispositius mòbils tant dins com fora de les instal·lacions de l'organització.
- Informació mentre s'accedeix a aquesta informació a través de dispositius que no són propietat de l'organització.

Aquesta política s'aplica a:

- Locals, instal·lacions i equips ubicats dins de l'IGTP.
- Dispositius de propietat personal que tenen la capacitat d'emmagatzemar, transferir o processar qualsevol informació sensible. Aquests dispositius inclouen ordinadors portàtils, telèfons intel·ligents, tauletes, memòries USB, càmeres digitals, etc.

Els usuaris d'aquest document són empleats de l'IGTP i personal adscrit.

1.1. Definicions

Dades Personals: qualsevol informació sobre una persona física identificada o identificable (l'interessat). S'ha de considerar persona física identificable qualsevol persona la identitat de la qual es pot determinar, directament o indirectament, en particular mitjançant un identificador, com per exemple un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona.

Categories especials de dades: dades personals que revelin l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques o l'afiliació sindical, i el tractament de dades genètiques, dades biomètriques destinades a identificar de manera unívoca una persona física, dades relatives a la salut o dades relatives a la vida sexual o les orientacions sexuals d'una persona física.

2. Confidencialitat i seguretat de dades personals i informació confidencial

2.1. Dades Personals

L'empleat i el personal adscrit, té l'obligació de tractar dades personals seguint el Reglament General de Protecció de Dades (2016/679).

L'empleat i el personal adscrit, també té l'obligació de mantenir la confidencialitat en relació amb les dades personals a les quals pot tenir accés per a la realització del seu treball, responsabilitat contractual o qualsevol altre tipus de responsabilitat i seguir les lleis aplicables, polítiques de privacitat i codi de conducta de l'IGTP.

2.2. Informació Confidencial

De la mateixa manera, i per garantir la confidencialitat i seguretat de la informació de l'activitat de l' IGTP, l'empleat i el personal adscrit es compromet a mantenir la confidencialitat en relació amb les dades personals a les quals pot tenir accés per a la realització del seu treball, responsabilitat contractual o qualsevol altre tipus de responsabilitat. L'empleat i el personal adscrit no utilitzarà cap informació confidencial a la qual tingui accés sota contracte per a finalitats diferents de les establertes en el seu contracte laboral, quedant expressament prohibida la divulgació d'informació confidencial.
Es considerarà informació confidencial, qualsevol informació (comercial, tècnica o d'altra índole), que pugui contenir dades personals o no, de l'IGTP i / o del client final, sobre els seus assumptes comercials, tecnologia, maquinària, processos, productes, plans , instal·lacions i dependències.
Dels esmentats en el paràgraf anterior, qualsevol informació que aparegui amb accés gratuït a la pàgina web del client, proveïdor o treballador no es considerarà informació confidencial.
També es considera altament confidencial, qualsevol informació que l'empleat i el personal adscrit pugui accedir a través dels sistemes informàtics de l'IGTP, els manuals tècnics que l'IGTP proporciona als empleats i el personal adscrit i la llista de clients de l'IGTP amb informació de contacte.

2.3. Mesures de Seguretat

2.3.1. Protegir informació confidencial o sensible

Abans de transferir o compartir informació confidencial i / o dades personals, els empleats i el personal adscrit han de protegir la informació. Protegir els fitxers amb una contrasenya abans de enviar o compartir els arxius serà considerada una mesura de seguretat adequada.

2.3.2. Dades Mèdiques

El personal de l'IGTP i el personal adscrit només podrà descarregar dades mèdiques no anònimes dins de l'entorn segur de les instal·lacions de l'IGTP. No es permet la descàrrega o la transferència de dades que continguin identificadors semi anònims en ordinadors personals o domèstics. Si les dades es baixen amb finalitats de còpia de seguretat, s'ha de fer directament en un sistema reconegut com segur (bloquejat, xifrat, etc.).
Si les dades s'han d'enviar fora de de l'IGTP, les dades mèdiques s'enviaran per correu electrònic protegides amb contrasenya mitjançant una plataforma de comunicació segura que permeti el xifratge i mai s'inclouran dades personals a l'assumpte o al text del correu electrònic.

2.3.3. Destrucció d'arxius que continguin dades personals i/o informació confidencial

Els documents que continguin informació confidencial es destruiran mitjançant una trituradora de documents o un altre servei de destrucció segura.
Tots els dispositius que continguin informació sensible i/o dades personals de categories especials que ja no s'utilitzin, es destruiran mitjançant un sistema de destrucció de dades certificat i segur.

3. Política de taula i pantalla neta

3.1. Protecció al lloc de treball

3.1.1. Política de taula neta

Si la persona autoritzada no està al seu lloc de treball, tots els documents en paper, així com els mitjans d'emmagatzematge de dades considerades sensibles, han de ser retirats de les taules de treball o d'altres llocs (impressores, màquines de fax, fotocopiadores, etc.) per evitar l'accés no autoritzat.

3.1.2. Política de pantalla neta

Si la persona autoritzada no està al seu lloc de treball, s'ha de treure de la pantalla tota la informació sensible i s'ha de prevenir l'accés a tots els sistemes per als quals la persona té autorització d'accés.
En cas d'absència curta (fins a 30 minuts), s'aplica la política de pantalla neta tancant la sessió de tots els sistemes o bloquejant la pantalla amb una contrasenya. En un sistema Windows, Windows_icon + L immediatament activa el protector de pantalla protegit per contrasenya.
Si la persona està absent durant un període de temps més llarg (més de 30 minuts), la política de pantalla neta s'implementa tancant sessió de tots els sistemes i apagant l'ordinador.

3.1.3. Contrasenyes

Tots els empleats i el personal adscrit, han de tenir contrasenya per accedir a:

1. Entorns i plataformes de treball
    - correu electrònic,
    - Espai de treball en Microsoft 365 y SAP
2. 2. Dispositius
    - Bloqueig de pantalla
    - Usuari informàtic

Les contrasenyes seran de caràcter unipersonal i confidencial i es modificaran, com a mínim, cada 180 dies.

3.2. Protecció d'instal·lacions i equipaments compartits

Els documents que contenen informació sensible han de ser eliminats immediatament de les impressores, fax i fotocopiadores.

4. Equip informàtic mòbil

4.1. Introducció

Els equips informàtics mòbils inclouen tot tipus d'ordinadors portàtils, telèfons mòbils, telèfons intel·ligents, targetes de memòria I d'altres equips mòbils utilitzats per a l'emmagatzematge, tractament i transferència de dades.

L'equip esmentat es pot treure fora del local només amb l'autorització del responsable del departament corresponent.

4.2. Normes bàsiques

Cal tenir especial cura quan l'equipament informàtic mòbil estigui ubicat en vehicles (inclosos els cotxes), espais públics, habitacions d'hotel, llocs de trobada, centres de conferències i altres àrees desprotegides fora de les instal·lacions de l'organització.

La persona que tregui equips informàtics mòbils fora de les instal·lacions ha de seguir les normes indicades a continuació:

- Els equips informàtics mòbils que portin informació confidencial, sensible o crítica no s'han de deixar sense vigilància i, si és possible, s'han de bloquejar físicament per assegurar l'equip.
- Quan s'utilitzin equips informàtics mòbils en llocs públics, l'usuari ha de tenir cura de que les dades no puguin ser llegides per persones no autoritzades
- La persona que utilitza equips informàtics mòbils fora de casa és responsable de les còpies de seguretat periòdiques de les dades.
- La informació sensible que hi hagi a ordinadors portàtils i USB s'ha de protegir amb contrasenya o xifrat.
- No emmagatzemar còpies locals de fitxers que continguin dades personals en dispositius portàtils, ja siguin personals o REDMO.

5. Teletreball

El treball fora de les instal·lacions de l'organització haurà d'estar autoritzat per Gerència

L'empleat s'encarregarà de garantir el següent:

- Protecció dels equips informàtics mòbils tal com s'especifica a la secció anterior
- Prevenció d'accés no autoritzat per persones que viuen o treballen en el lloc on es realitza l'activitat de teletreball
- Configuració adequada de la xarxa local utilitzada per connectar-se a Internet
- Protecció dels drets de propietat intel·lectual de l'organització, ja sigui per a programari o altres materials que es puguin protegir mitjançant drets de propietat intel·lectual
- Devolució i eliminació de dades i equips en cas d'extinció de contracte.

6. Ús de dispositius propis

6.1. Normes per garantir la seguretat en l'ús de dispositius propis

Les normes d'aquesta política s'apliquen a tots els dispositius propis, tant si són utilitzats per a treballs com per a ús privat, o si s'utilitzen dins o fora de les instal·lacions de l'organització.

6.1.1. Política de l'organització

L'IGTP admet l'ús de dispositius propis per realitzar treballs per a l'empresa, dins les restriccions que l'IGTP contempla en aquests casos. Això vol dir, incapacitat de connexió a la xarxa interna (només connexió a wifi de convidat), entre d'altres exposats a la normativa IT.
Les dades de l'empresa emmagatzemades, transferides o processades als dispositius propis es mantenen sota la propietat de l'empresa i l'empresa es reserva el dret de controlar aquestes dades encara que no sigui el propietari del dispositiu.

7. Comentaris o Preguntes

Si teniu comentaris o preguntes sobre aquesta política de seguretat, envieu-les a dpd@igtp.cat

8. Referències

- REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU I DEL CONSELL, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades)
- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals
- Política de Privacitat de l'IGTP: http://www.germanstrias.org/es-legal-notice/