Secretaria General
Servei de Secretaria General i Serveis Jurídics
ORD.GEN 2023003

ANUNCI SOBRE L'APROVACIÓ DEFNITIVA DEL REGLAMENT D'ÚS DE DADES I DELS SISTEMES D'INFORMACIÓ DE L'AJUNTAMENT DE MANRESA

El Ple Municipal de l'Ajuntament de Manresa, en sessió del dia 21 de març de 2024, va adoptar, entre d'altres, l'acord relatiu a aprovar inicialment el nou *Reglament d'ús de dades i de sistemes d'informació de l'Ajuntament de Manresa* i va sotmetre l'expedient a informació pública per un període de trenta dies hàbils.

Transcorregut aquest termini sense que s'hagin presentat al·legacions, l'acord inicial ha esdevingut definitiu, per la qual cosa, es fa públic el text íntegre del nou *Reglament d'ús de dades i dels sistemes d'informació de l'Ajuntament de Manresa*, que s'insereix a continuació, per al seu general coneixement i en compliment del que es disposa en l'article 70.2 de la Llei 7/1985, de 2 d'abril, Reguladora de les Bases del Règim Local, en relació amb l'article 66.1 del Reglament d'obres, activitats i serveis dels ens locals aprovat per Decret 179/1995, de 13 de juny.

Aquest reglament entrarà en vigor un cop hagi estat publicat íntegrament al Butlletí Oficial de la Província de Barcelona i sempre que hagi transcorregut el termini de 15 dies a què fa referència l'article 65.2 de la Llei 7/1985, de 2 d'abril, reguladora de les bases de règim local.

Contra aquest acord, que és definitiu en via administrativa, els interessats poden interposar recurs contenciós administratiu davant la Sala del contenciós administratiu del Tribunal Superior de Justícia de Catalunya, en el termini de dos mesos a comptar des de l'endemà de la data de la seva publicació.

L'alcalde,

REGLAMENT D'ÚS DE LES DADES PERSONALS I ELS SISTEMES D'INFORMACIÓ

Aquest document detalla les funcions i obligacions del personal de l'Ajuntament de Manresa i del personal i entitats externes a l'Ajuntament respecte a l'ús de les dades personals i els sistemes d'informació.

Contingut

Reglament d'ús de les dades personals i els sistemes d'informació

Preàmbul

Les tecnologies de la informació i de la comunicació han de ser utilitzades per millorar la qualitat i l'accessibilitat dels serveis públics, per interaccionar amb la ciutadania, amb altres administracions i amb els sectors directament relacionats, i per facilitar alhora la transparència i el retiment de comptes de les administracions.

Aquests recursos han de ser orientats envers els processos de gestió, redefinint-los i simplificant-los quan calgui, per tal de millorar-ne l'eficiència.

L'ús dels sistemes d'informació ha de ser curós amb l'estricte compliment de la normativa vigent que els regula. En aquest sentit, a l'Ajuntament de Manresa la utilització dels mitjans electrònics se sotmet a les limitacions establertes en la Constitució i en la resta de l'ordenament jurídic estatal i autonòmic, amb ple respecte als drets que les persones tenen reconeguts. En especial, s'haurà d'actuar de conformitat amb el que estableixen l'article 18.4 de la Constitució, la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de dades de personals i garantia dels drets digitals, la Llei 32/2010, d'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, i la resta de normes específiques que regulen el tractament de la informació.

Aquest Reglament pretén establir els criteris generals per a l'ús adequat de les dades de caràcter personal i dels recursos i sistemes d'informació de l'Ajuntament de Manresa i donar normes i recomanacions per fer conscients a tots els servidors i servidores públiques de la importància de fer-ne un ús responsable a tots els nivells.

1. Glossari

- API. De l'anglès Aplication Programming Interface, (interfície de programació d'aplicacions). La funció és permetre a diferents aplicacions comunicar-se entre elles i compartir informació i funcionalitats.
- Credencials. Sistemes que permeten a una persona usuària accedir a un determinat entorn de treball de manera que el seu accés sigui degudament identificat i registrat. Poden estar compostos d'un número identificador i contrasenya, o certificat digital.
- Enviament telemàtic. Enviament de documents electrònics a tercers que no estigui relacionat amb notificacions electròniques o trameses a altres administracions públiques.
- Incident de seguretat. Situació sobrevinguda produïda en el tractament de la informació que impedeix accedir a la informació (disponibilitat), que suposa una divulgació no autoritzada d'informació confidencial (confidencialitat), o una pèrdua d'informació (integritat).
- Núvol corporatiu. És l'eina corporativa habilitada per l'Ajuntament per a la realització d'enviaments telemàtics a tercers.
- Persones usuàries. Són les persones que es relacionen a l'article 3 del present Reglament.
- Responsable de Seguretat. És un òrgan col·legiat format pel Servei de cooperació en l'Administració electrònica, Transparència i Protecció de Dades, el Servei d'Organització i Recursos Humans i el Servei de Tecnologies i Sistemes de la Informació que

s'encarrega de definir aquells protocols i mesures per tal de garantir la seguretat de la informació. El mecanisme de comunicació amb el Responsable de Treball és l'adreça de correu electrònic.

- Servei de Tecnologies i Sistemes d'Informació. És el servei de l'Ajuntament que s'encarrega de la gestió dels sistemes informàtics corporatius, sent el responsable de tramitar totes les sol·licituds relacionades amb aquests.
- Sistemes d'informació. Els Sistemes d'Informació de l'Ajuntament comprenen qualsevol equipament informàtic (ordinador de sobretaula, ordinador portàtil, telèfon intel·ligent, tauleta, perifèrics, dispositius d'impressió) i servei de xarxa (correu electrònic, internet, comunicacions, programari) facilitat per l'Ajuntament per al desenvolupament de les seves funcions.
- Unitat local. Unitat d'emmagatzematge local dels equips informàtics assignats.
- Xarxa corporativa. Conjunt de carpetes compartides entre les persones usuàries d'un Servei o entre diferents Serveis de l'Ajuntament, on les persones usuàries emmagatzemen els fitxers informàtics utilitzats per al desenvolupament de les funcions associades al lloc de treball.

2. Objecte

Aquest Reglament té per objecte regular l'ús de les dades personals i els sistemes de la informació en l'àmbit de l'Ajuntament de Manresa i el seu sector públic.

3. Marc normatiu

El Reial decret 311/2022, de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat (ENS) estableix la necessitat de disposar d'una normativa interna que reguli la utilització dels sistemes d'informació per part del conjunt de les persones usuàries de l'Ajuntament. Aquesta obligació es materialitza a l'article 15 d'aquest RD on s'estableix la necessitat que l'entitat estableixi una normativa de seguretat que defineixi les directrius per garantir un ús segur dels sistemes d'informació per part de les persones usuàries.

En compliment d'aquesta obligació i amb l'objectiu de garantir un ús adient dels sistemes d'informació i de les dades de caràcter personal, l'Ajuntament de Manresa defineix les següents obligacions per al conjunt de persones usuàries.

3.1. Normativa a aplicar

La legislació sobre protecció de dades de caràcter personal i sobre la seguretat de la informació, constitueixen el marc jurídic per les normes d'ús del sistema informàtic i de comunicacions que s'incorporen en aquest document. Les principals referències legals són les següents:

3.1.1. Llei Orgànica 3/2018, de 5 de desembre, de Protecció de dades de personals i garantia dels drets digitals (LOPD). L'article 5 estableix el deure de confidencialitat i secret professional a tota persona que intervingui en qualsevol fase del tractament de les dades de caràcter personal i el deure de guardar-ho. Aquesta obligació que s'estén més enllà de la durada de la relació de la persona amb l'ens,

3.1.2. Reial decret legislatiu 1/1996, de 12 d'abril, per al que s'aprova el text refós de la Llei de Propietat Intel·lectual (LPI).

3.1.3. Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'Àmbit de l'Administració Electrònica.

3.1.4. Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.

3.1.5. Reial decret 311/2022, de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat (ENS).

3.1.6. Normativa bàsica de protecció de la informació del CCN (Centro Criptológico Nacional).

3.1.7. Normativa del Pla nacional de seguretat d'impuls de la seguretat TIC a Catalunya aprovat per al Govern de la Generalitat el 17 de març del 2009, per la implantació de la seguretat de la informació es disposa del suport del Centre de Seguretat de la Informació de Catalunya (CESICAT).

3.1.8. El conjunt d'Instruccions de l'Agència Catalana de Protecció de Dades.

3.1.9. Reglament (UE) 910/2014 del Parlament Europeu i del Consell de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior, i pel que es deroga la Directiva 1999/93/CE (ReIDAS).

4. Àmbit d'aplicació

El present Reglament és d'aplicació a la totalitat de les persones que prestin serveis a l'Ajuntament de Manresa i el seu sector públic (d'ara endavant persones usuàries) amb accés a les dades confidencials i personals responsabilitat de l'entitat (càrrecs electes, funcionaris/àries i personal assimilat).

Tot el personal al servei de l'Ajuntament de Manresa que, per raons de les seves funcions tingui accés a la utilització de tecnologies de la informació i la comunicació (correu electrònic, internet, intranet, aplicacions internes, etc.), queda inclòs dins l'abast de l'aplicació d'aquest document. També els serà d'aplicació a aquelles persones, que sense mantenir una vinculació laboral amb l'Ajuntament de Manresa, realitzin funcions de gestió i manteniment dels sistemes informàtics i de comunicacions de dades.

5. Obligacions de les persones usuàries

5.1. General

5.1.1. L'Ajuntament facilitarà a les persones usuàries l'equipament informàtic (ordinador de sobretaula, ordinador portàtil, telèfon intel·ligent, tauleta, perifèrics, dispositius d'impressió) i els serveis de xarxa (correu electrònic, internet, comunicacions, programari) que siguin necessaris per a la realització de les tasques professionals relacionades amb el seu lloc de treball a les dependències municipals.

5.1.2. Aquests equipaments són propietat de l'Ajuntament i la seva utilització es limitarà exclusivament a aquelles accions necessàries per portar a terme les seves tasques professionals.

5.1.3. L'Ajuntament posa a disposició de les persones usuàries, xarxes de wifi amb la finalitat que puguin connectar dispositius a la xarxa per desenvolupar tasques relacionades amb l'Ajuntament com reunions o formacions telemàtiques, també es poden connectar a aquestes xarxes altres dispositius personals, sempre que se'n faci un ús responsable. Aquestes xarxes estan publicades a la Intranet.

5.1.4. Les tasques professionals a les dependències municipals s'hauran de realitzar amb els equips informàtics corporatius, qualsevol excepció a aquesta situació haurà de ser autoritzada per la persona Responsable de Seguretat.

5.1.5. Els equipaments hauran de ser retornats a l'Ajuntament un cop finalitzada la prestació de serveis en les mateixes condicions en què va ser facilitat.

5.1.6. L'Ajuntament es reserva el dret de fer un seguiment de l'ús d'aquestes eines amb aquells mitjans disponibles amb l'objectiu que se'n faci un ús adequat d'acord amb el desenvolupament de les tasques professionals, respectant en tot cas el dret a la intimitat, a l'honor i a la privacitat de les persones usuàries.

5.1.7. Els sistemes d'informació posen a l'abast de les persones usuàries uns procediments de gestió d'incidències a través de les aplicacions de la intranet per tal de poder fer un correcte seguiment i atenció i resolució d'aquestes. El procediment principal és el CIM.INF.

5.2. Deure de secret

Les persones usuàries del sistema d'informació municipal hauran de mantenir el deure de secret i guardar, per temps indefinit, la màxima reserva en relació amb les dades, els documents, les metodologies, les claus, l'anàlisi, els programes i la resta d'informació als quals tinguin accés durant la seva relació laboral amb l'Ajuntament de Manresa. Aquesta obligació continuarà vigent després de l'extinció de la seva vinculació professional, particularment en relació amb tot el referent als fitxers de dades personals.

Els usuaris seran responsables de la utilització de la informació confidencial i de caràcter personal a la qual tinguin accés i de mantenir la qualitat d'aquestes.

S'entendrà per informació confidencial, tota aquella informació que contingui dades personals, com també tota aquella informació de caràcter rellevant per l'Ajuntament.

La qualitat de les dades ha de ser entesa com:

- L'adequació de les dades a la finalitat per la qual es van recollir, sol·licitant només les dades estrictament necessàries i legítimes per la prestació del servei.
- L'ús legítim i lícit de les dades d'acord amb la finalitat per la qual es van recollir.
- L'exactitud, fiabilitat i veracitat de les dades.

Quan la persona usuària estimi que es pot produir una cessió de dades de caràcter personal, haurà de tramitar l'autorització expressa del responsable del fitxer, en els supòsits legalment admissibles, a través del procediment AJT.SDP (seguretat de dades personals)

Aquesta és la normativa a aplicar en l'ús de les dades:

5.2.1. No està permès transmetre informació confidencial de l'Ajuntament a l'exterior mitjançant suports materials o qualsevol altre mitjà de transmissió, inclosos la simple visualització o l'accés per part de tercers, amb l'excepció que es compti amb autorització expressa del/de la Responsable del Tractament.

5.2.2. En el cas que, per motius directament relacionats amb el desenvolupament de les seves funcions, la persona usuària entri en possessió d'informació confidencial en qualsevol mena de suport, caldrà entendre que aquesta possessió és estrictament temporal, sense que l'expressada circumstància li atorgui cap dret possessori, titularitat o dret de còpia de l'esmentada informació.

5.2.3. D'aquesta manera, l'usuari haurà de retornar els citats materials a l'Ajuntament o destruir-los immediatament després de la finalització de les tasques que han originat el seu ús temporal i, en qualsevol cas, en la finalització de la vinculació amb l'entitat.

5.2.4. L'Ajuntament inclourà clàusules legals en la formalització de la relació amb les parts contractades que el vinculin, amb l'objectiu que aquests siguin obligats a mantenir el deure de secret respecte les dades de caràcter personal a les quals tinguin accés en virtut de l'encàrrec que se'ls realitzi, fins i tot després que finalitzi el seu objecte.

5.2.5. L'incompliment del deure de secret pot constituir un delicte de revelació de secrets dels previstos en els articles 195,197 al 201 del Codi Penal.

5.3. Utilització de credencials (identificador i clau d'accés) i certificats digitals

Disposar de credencials per l'accés al sistema informàtic és una acció necessària per a protegir la informació corporativa i evitar que algú, de forma no legítima, tingui accés a uns recursos que no li corresponen.

5.3.1. Al personal de l'Ajuntament que en funció del seu lloc de treball requereixin tenir accés al sistema informàtic, se'ls facilitarà les credencials per l'ús dels equips i aplicacions corporatives assignats. Aquest codi es facilitarà en el moment en què des del Servei d'Organització i Recursos Humans enregistrin l'alta a través d'un procediment SGI.ACD i després del vistiplau del corresponent cap de servei.

5.3.2. Les credencials, certificats digitals són personals i intransferibles. Està expressament prohibit comunicar, compartir o deixar a l'abast els certificats digitals o contrasenyes d'accés als serveis telemàtics de la xarxa corporativa. En cas d'incompliment d'aquesta prohibició, l'usuari serà l'únic responsable de les conseqüències que es puguin derivar del mal ús, la divulgació o la pèrdua d'aquestes.

5.3.3. Per tal de garantir la confidencialitat de les credencials, cada persona usuària serà responsable d'emprar contrasenyes que no siguin fàcilment deduïbles, serà obligatori canviar la contrasenya inicial temporalment assignada durant la primera connexió al sistema i

canviar-la cada tres mesos atenent les notificacions del sistema i davant de qualsevol sospita d'incident de suplantació d'identitat de l'usuari.

5.3.4. Referent a l'ús de contrasenyes s'han de tenir en compte els següents punts:

5.3.4.1. Per tal de millorar la fortalesa de la contrasenya, serà exigible que tingui números, lletres majúscules, minúscules i caràcters especials (*, +, $, %, &, @, !, ...). El sistema exigirà una contrasenya de mínim 8 caràcters.

5.3.4.2. Les contrasenyes no es poden enviar per correu electrònic o mitjançant altres serveis telemàtics sense xifrar. Els procediments operacionals poden requerir compartir les contrasenyes amb els Administradors del sistema. Un cop finalitzada l'assistència, l'usuari és responsable de canviar la contrasenya. Això és acceptable només en les circumstàncies següents:

5.3.4.2.1. Amb autorització prèvia de l'interessat.

5.3.4.2.2. En presència de l'interessat.

5.3.5. Es permet un màxim de tres intents de connexió. En el cas de no haver aconseguit entrar, el compte de la persona usuària queda bloquejat/revocat i cal contactar amb el servei Tecnologies i Sistemes d'Informació per tornar a activar-lo.

5.3.6. Si un usuari sospita que han estat vulnerades les seves dades d'identificació i d'accés, o bé hagués oblidat la seva contrasenya, serà necessari comunicar aquesta situació al Servei de Tecnologies i Sistemes d'Informació per tal que procedeixi a la corresponent anàlisi i a reiniciar les credencials. Aquesta comunicació/petició es farà mitjançant el procediment CIM.INF.

5.3.7. Davant una baixa o absència temporal d'una persona usuària, no es podrà utilitzar la seva identificació i contrasenya per accedir al seu equip. En cas que sigui necessari, el/la seu/va cap haurà de sol·licitar-ho al departament de Tecnologies i Sistemes d'Informació mitjançant el procediment CIM.INF i se'n donarà comptes al Comitè de Seguretat. En aquest cas no serà necessari el consentiment de la persona usuària.

5.3.8. Quan una persona usuària deixi de prestar els seus serveis a l'Ajuntament, el seu identificador i contrasenya quedarà inutilitzat, des del moment que el departament de RRHH ho comuniqui al Servei de Tecnologies i Sistemes d'Informació a través del corresponent procediment SGI.ACD.

5.3.9. Per tal de garantir la protecció de les credencials d'accés a serveis telemàtics es recomana no emmagatzemar credencials a les

aplicacions i no mantenir les sessions iniciades quan no es requereixin.

5.3.10. És aconsellable fer servir contrasenyes diferents per cada àmbit. Si tenim una contrasenya per al correu corporatiu i una altra per l'accés a les aplicacions i una de les dues contrasenyes es veu compromesa, l'altra continuarà sent segura.

5.3.11. S'aconsella no fer servir la mateixa contrasenya que es fa servir a l'organització en sistemes administrats per altres organitzacions.

5.3.12. Les condicions i recomanacions definides per a credencials en aquest apartat afecten les credencials els sistemes propis de l'Ajuntament com aquelles credencials generades en plataformes de tercers que siguin utilitzades per les persones usuàries en el desenvolupament de les seves funcions professionals.

5.3.13. L'Ajuntament de Manresa defineix com eines corporatives per a la gestió de les contrasenyes l'aplicació PSONO i el Gestor de contrasenyes de Google.
A aquestes eines s'hi pot accedir des d'internet i permeten emmagatzemar les diferents contrasenyes de les persones usuàries. Per fer ús de l'eina PSONO és requisit indispensable que s'activi l'autenticació amb doble factor i que s'utilitzi una contrasenya complexa, de com a mínim 16 caràcters de longitud que contingui com a mínim caràcters de dos dels següents tipus: lletres majúscules, lletres minúscules, números o símbols.

5.4. Utilització de la xarxa corporativa

5.4.1. Tota la informació generada per les persones usuàries de l'Ajuntament haurà de ser emmagatzemada a la unitat corresponent de la xarxa corporativa.

5.4.2. La xarxa corporativa de l'Ajuntament es compon pels següents grups de carpetes, en funció de la seva funcionalitat:

5.4.2.1. P: Unitat d'emmagatzematge Personal, que té com a finalitat la de servir d'emmagatzematge d'aquella informació personal relativa al servei prestat a l'Ajuntament. Cada usuari disposa d'una unitat P i és l'única persona usuària que hi té accés.

5.4.2.2. Q: Unitat d'emmagatzematge Comú d'informació dels Serveis municipals, que té com a finalitat l'emmagatzematge de la informació de treball dels Serveis de l'Ajuntament. Cada departament/àmbit disposa d'una unitat Q i totes les persones usuàries del departament/àmbit hi tenen accés.

5.4.2.3. X: Unitat d'emmagatzematge d'informació d'ArXiu dels Serveis municipals, que té com a finalitat l'emmagatzematge de la informació històrica dels Serveis de l'Ajuntament. Cada departament/àmbit disposa d'una unitat X i totes les persones usuàries del departament/àmbit hi tenen accés.

5.4.2.4. T: Unitat de Traspàs. Unitat que té com a finalitat exclusiva la de servir com a espai per compartir informació entre els diferents Serveis i persones usuàries de l'Ajuntament.

5.4.3. Les dades corporatives i la informació de treball de cada servei hauran de ser emmagatzemades a les unitats Q i X assignades pel Servei de Tecnologies i Sistemes d'Informació. En cap cas aquesta informació podrà ser emmagatzemada a la Unitat P assignada a l'usuari.

5.4.4. Aquelles persones usuàries que utilitzin la unitat T per compartir informació hauran de garantir que aquesta no sigui conservada en aquesta unitat, en tractar-se d'una unitat amb l'única finalitat de compartir informació. La informació que resti emmagatzemada en aquesta unitat serà esborrada setmanalment.

5.4.5. El Servei de Tecnologies i Sistemes d'Informació realitza còpies diàries de les unitats personals (P) i compartides (Q i X).

5.4.6. Les unitats locals dels equips assignats als usuaris per portar a terme la seva tasca dins de l'Ajuntament no són en cap cas unitats d'emmagatzematge d'informació. L'Ajuntament no podrà garantir la recuperació de la informació emmagatzemada en aquestes unitats en cas d'incidència.

5.4.7. Les unitats P, Q, X, T i els servidors externs ubicats al núvol són per l'emmagatzematge exclusiu d'informació relacionada amb l'activitat de l'Ajuntament. No està permès emmagatzemar altre tipus de continguts en aquestes unitats.

5.4.8. En cas que sigui necessari per a les funcions del servei el tractament d'imatges caldrà utilitzar la unitat habilitada per l'Ajuntament per l'emmagatzematge d'aquest tipus de fitxers.

5.4.9. El tractament de la informació emmagatzemada al núvol corporatiu s'haurà de portar a terme respectant les mateixes mesures de seguretat i confidencialitat que l'accés a informació en els servidors corporatius. Així mateix, la informació que s'hi guardi i es comparteixi, es tractarà d'acord amb els protocols de seguretat adients. En aquest sentit, l'Ajuntament de Manresa disposa d'una instrucció en la qual es defineixen els criteris a tenir en compte i la casuística en què de forma excepcional es podrà guardar i compartir documentació municipal al núvol.

5.4.10. No està permès l'emmagatzematge o transmissió d'informació corporativa a sistemes de núvols no autoritzats per l'Ajuntament de Manresa.

5.4.11. No està permès l'emmagatzematge o transmissió d'informació corporativa a sistemes d'emmagatzematge extern com USB o discos extraïbles.

5.5. Ús del correu electrònic corporatiu

La finalitat del correu electrònic és proporcionar una comunicació entre persones, siguin o no de l'organització municipal. Un ús d'aquest mitjà sense observar les degudes mesures de seguretat pot tenir un impacte negatiu econòmic, legal i d'imatge per l'organització.

Els criteris per l'ús del correu electrònic corporatiu són els següents:

5.5.1. Es considerarà correu electrònic corporatiu qualsevol adreça electrònica corporativa generada dins dels dominis de l'Ajuntament.

5.5.2. L'Ajuntament assignarà un compte de correu electrònic personal per cada usuari. Aquest, serà personal i intransferible.

5.5.3. Sempre que L'Ajuntament de Manresa hagi d'enviar un correu electrònic al seu personal, ho farà utilitzant els comptes de correu corporatius.

5.5.4. El personal de l'Ajuntament de Manresa té l'obligació de consultar el seu compte de correu corporatiu amb regularitat.

5.5.5. El servei de correu electrònic corporatiu haurà de ser utilitzat per a finalitats directament relacionades amb les funcions desenvolupades a l'Ajuntament, per a la comunicació d'aspectes relacionats amb el desenvolupament de la feina diària i/o el compliment de les obligacions laborals.

5.5.6. No està permesa la utilització del compte de correu electrònic corporatiu per registrar-se en serveis que no estiguin directament relacionats amb les funcions desenvolupades a l'Ajuntament. Per exemple comptes personals d'Instagram, Twitter, comptes bancaris, etc.

5.5.7. Les adreces genèriques de cada àrea seran responsabilitat del seu/de la seva cap, sent aquest/a l'encarregat/ada de regular i definir la seva utilització. En tot cas, aquests comptes no podran ser utilitzats com a bústia de correu electrònic personal dels usuaris.

5.5.8. El servei de correu electrònic corporatiu haurà de ser emprat per finalitats directament relacionades amb les funcions desenvolupades a l'Ajuntament, per la comunicació d'aspectes relacionats amb el desenvolupament de la feina diària i/o el compliment de les respectives funcions assignades.

5.5.9. No es podran descarregar fitxers des del compte de correu electrònic, que no tinguin relació amb les funcions desenvolupades a l'Ajuntament. Concretament, les persones usuàries hauran d'estar alerta, entre altres coses, d'aquells correus rebuts de persones o entitats conegudes que s'expressin en idioma estranger, o bé amb correus amb fitxers adjunts que no hagin estat sol·licitats prèviament o correus amb un assumpte no definit.

5.5.10. S'estableix l'obligació per part de l'usuari de no obrir correus d'origen desconegut i de contingut sospitós. En cas que sigui sospitós, es

comunicarà al Servei de Tecnologies i Sistemes d'Informació amb la màxima celeritat.

5.5.11. En cas d'una absència programada (vacances, permisos...) la persona usuària serà responsable de programar una autoresposta al seu compte de correu electrònic informant d'aquesta situació. El text programat a l'autoresposta serà definit per la mateixa persona usuària, podent indicar una adreça de correu electrònic al qual les persones es puguin dirigir durant la seva absència. En cas que a causa de l'absència no permeti configurar-ho ell mateix, el Servei de Tecnologies i Sistemes d'Informació ho resoldrà a instància de la prefectura del servei. En aquells casos que la persona usuària no ho hagi requerit, el Responsable de Seguretat podrà determinar la necessitat d'activar-ho.

5.5.12. Queda prohibida la difusió massiva i genèrica de comunicats, notícies o informació de qualsevol caràcter que no estiguin relacionats amb l'activitat de l'Ajuntament. La difusió de la informació d'interès general per al conjunt de l'Ajuntament s'efectuarà a través dels canals habilitats de difusió d'informació.

5.5.13. Quan una persona usuària deixa de prestar els seus serveis a l'Ajuntament, el seu identificador i contrasenya queden inutilitzats des del moment que el Servei d'Organització i Recursos Humans ho comuniqui al Servei de Tecnologies i Sistemes d'Informació a través del corresponent procediment SGI.ACD. Tot i que les credencials quedin bloquejades, es mantindrà durant un mes la bústia personal de la persona usuària, en previsió de necessitats del servei al qual estava adscrit o per motius legals. Passat aquest mes s'eliminarà el compte.

5.5.14. En cas que sigui necessari accedir al correu electrònic de la persona usuària, el/la seu/va cap haurà de sol·licitar-ho al Servei de Tecnologies i Sistemes d'Informació mitjançant el procediment CIM.INF i se'n donarà comptes al Comitè de Seguretat. En aquest cas serà necessari el consentiment de la persona usuària.

5.5.15. En el cas que es detectin indicis fonamentats d'un ús inadequat del correu electrònic corporatiu, l'Ajuntament podrà dur a terme un seguiment per la seva adequada utilització.

5.5.16. A la Intranet municipal hi constaran recomanacions tècniques i enllaços o guies d'ús publicades per CESICAT o altres organismes de seguretat.

5.5.17. Els comptes d'usuari de correu electrònic corporatiu seguiran per defecte l'estructura [nom].[cognom]@ajmanresa.cat, podent-se modificar en el cas que hi hagi duplicitats o per conveniència justificada de l'usuari. En cas de col·lectius sensibles (per exemple Policia Local o Serveis Socials), es podran crear àlies que anonimitzin l'adreça de correu.

5.6. Treball fora de les dependències de l'Ajuntament (teletreball)

5.6.1. La realització del teletreball estarà subjecte a totes les normes especificades al reglament de teletreball que aprovi l'Ajuntament de Manresa.

5.6.2. L'Ajuntament habilitarà accessos remots pel treball fora de les dependències de l'Ajuntament a aquelles persones usuàries que ho precisin pel desenvolupament de les seves funcions, sempre que ho autoritzi el seu cap de servei d'acord amb la regulació interna de l'Ajuntament.

5.6.3. Els accessos remots als sistemes corporatius es realitzaran exclusivament amb els equips que disposin d'accés remot configurat pel Servei de Tecnologies i Sistemes d'Informació, la utilització d'altres mitjans haurà de ser autoritzada per la Comissió de Seguretat.

5.6.4. Les persones usuàries hauran de respectar les mesures de seguretat establertes per tal de garantir que el treball fora de les dependències municipals es presti amb un nivell de mesures de seguretat concurrent amb la normativa vigent en matèria de seguretat de la informació.

5.7. Utilització de dispositius d'emmagatzematge extern

5.7.1. No està permesa la utilització de dispositius d'emmagatzematge extern (dispositius de memòria USB o similars) per la càrrega i la descàrrega de continguts de la Xarxa Corporativa, llevat d'aquells casos concrets que siguin autoritzats per la Comissió de Seguretat.

5.7.2. En cas de comptar amb autorització caldrà utilitzar els dispositius externs validats pel Servei de Tecnologies i Sistemes d'Informació.

5.7.3. No està permesa la connexió a la xarxa corporativa de dispositius d'aquestes característiques bé siguin personals o de persones usuàries externes a l'organització. En els casos que sigui indispensable, es farà en els equips destinats a aquesta funció i aprovats per la Comissió de Seguretat.

5.8. Enviaments de dades per mitjans telemàtics

S'entén com a enviament d'informació per mitjans telemàtics qualsevol transmissió de dades personals responsabilitat de l'Ajuntament fora de la xarxa corporativa, llevat d'aquelles comunicacions a altres administracions públiques que es realitzaran mitjançant les plataformes habilitades i les notificacions electròniques.

5.8.1. Les transmissions de dades fora de la xarxa corporativa hauran de ser realitzades mitjançant el núvol corporatiu habilitat per Sistemes d'Informació, no està permesa la transmissió de dades de caràcter personal amb qualsevol altre tipus d'eina (correu electrònic personal, xarxes socials, aplicacions de xat o núvols de tercers).

5.8.2. No es podran efectuar enviaments ni recepcions d'informació mitjançant dispositius i mitjans que no siguin els proporcionats per l'Ajuntament i aprovats per la Comissió de Seguretat. (Exemple de

dispositius o mitjans no permesos: USB particulars, telèfons particulars, Whatsapp personal, aplicacions de transferència de fitxers tipus filetransfer, correu electrònic personal, serveis d'edició de documents PDF on-line, ILovePDF,...).

5.8.3. Per dur a terme descàrregues per altres tipus de plataformes diferents de les corporatives, caldrà sol·licitar-ho al del Servei de Tecnologies i Sistemes d'Informació mitjançant un procediment CIM.INF.

5.9. Espai de treball al núvol

A través d'un contracte obert, l'Ajuntament de Manresa ha optat per la solució de Google Workspace (Drive) per implantar i posar en marxa el sistema de correu, emmagatzematge i gestió de fitxers al núvol, amb l'objectiu de cobrir la creació dels seus comptes d'usuari, l'habilitació i configuració dels serveis de gestió de fitxers i la formació i suport dels administradors i usuaris, quedant fora de l'abast qualsevol migració de dades.

La solució adquirida disposa d'una consola per donar d'alta i permisos als usuaris així com extreure informes d'auditoria i logs. També s'inclouen sessions de formació als usuaris per a una correcta utilització accessible total o parcialment als usuaris de l'entorn amb els permisos assignats per a ells que permeten l'administració completa de l'entorn (gestió de persones usuàries i grups, gestió dels serveis, configuració del compte i seguretat) així com accés als informes d'ús eines d'auditoria i logs.

Permet operar de manera similar mitjançant les APIs pròpies dels serveis per automatitzar o realitzar accions de forma programàtica. Aquestes accions estan disponibles tant per a funcions d'administració com per als serveis de treball amb documents o emmagatzematge.

Aquest espai és un entorn col·laboratiu de computació al núvol que permet crear i compartir carpetes i documents de diferents tipus (textos, presentacions, imatges, fulls de càlcul, etc.) entre diverses persones usuàries. Les aplicacions ofimàtiques associades permeten editar els documents tant individualment com simultàniament entre diversos usuaris, compartir comentaris, controlar les versions i exportar-los a altres formats (PDF, Word, PPT, etc.).

La utilització de l'espai al núvol (Drive) és el mètode recomanat, alternatiu als dispositius de memòria externs (USB, discs…), per l'emmagatzematge d'arxius que provinguin de fonts externes o als que s'hagi d'accedir des de fora de l'Ajuntament.

L'accés al compte corporatiu que dona accés a la plataforma tindrà les següents característiques:

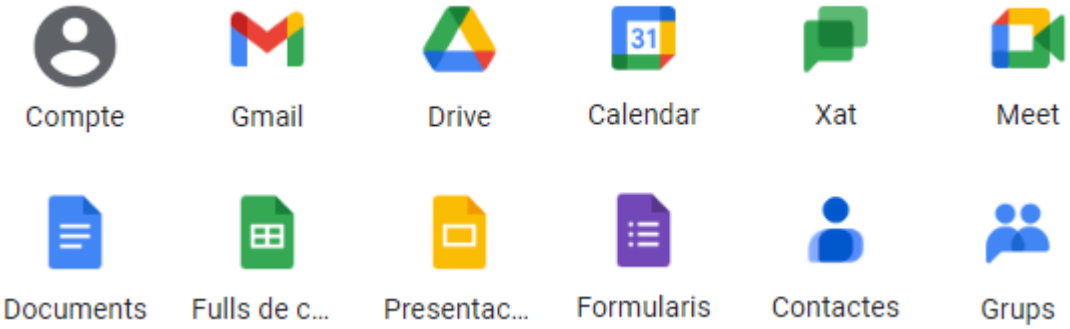
-El compte de persona usuària haurà de tenir una contrasenya de mínim 8 caràcters amb complexitat.

-La contrasenya tindrà una caducitat de 90 dies.

-La màxima durada de sessions sense activitat durant un període de 14 dies, seran tancades automàticament.

5.9.1. Eines

Es posa a disposició del personal de l'Ajuntament les eines del Google Workspace que, entre d'altres, són les següents:



Les eines com el Xat, que permeten un treball col·laboratiu de manera fàcil i àgil dins d'un grup o departament, en cap cas són les eines indicades per comunicar incidències o peticions a altres serveis, que s'hauran de fer pels canals preparats a tal efecte, per exemple els procediments CIM.INF, SGI.ACD, MAN.EDI, etc.

5.9.2. Missió

L'espai de treball al núvol permet el treball de forma individual (crear un document, editar-lo i emmagatzemar-lo) des de diferents ubicacions, sense haver de guardar el document en el disc dur de l'ordinador, aspecte molt adequat i que facilita el teletreball. Alhora, també permet l'opció d'un treball col·laboratiu, si és necessari, que fomenta la participació i contribueix a desenvolupar la capacitat de treball en equip, la presa conjunta de decisions i la construcció col·laborativa de coneixement.

5.9.3. Permisos d'accés

L'Ajuntament no permetrà mai el lliure accés a les seves carpetes i arxius. Quan l'Ajuntament comparteixi informació amb una persona usuària haurà de tenir en tot moment coneixement de què és el que comparteix, quan i com. Aquest coneixement no constitueix només una mesura, és seguretat plena, i també proporciona un control sobre la informació.

En aquest sentit, el programari disposa de gestió de persones usuàries i permisos d'accés. Sobre aquestes persones usuàries es podrà concedir o denegar permisos d'accés en qualsevol moment. L'Ajuntament no permetrà compartir arxius de forma lliure i mitjançant enllaços.

Cap persona usuària podrà decidir guardar dades al núvol de forma personal i autònoma, sense el coneixement i consentiment del seu cap de servei. En aquest sentit, l'Ajuntament facilitarà la possibilitat de donar d'alta a la plataforma a les persones usuàries designades pels/per les respectius/ives caps de servei, que rebran la corresponent formació.

L'Ajuntament a través de la present instrucció fa extensiva a totes les persones usuàries l'exigència de què en el núvol només s'hi pot guardar informació relacionada amb les tasques pròpies del lloc de treball assignat, i en cap cas documentació de l'esfera personal o privada.

5.9.4. Control d'accions

Quan l'Ajuntament utilitzi algun programari d'ús d'arxius haurà de conèixer què ha passat a la vida d'aquests arxius. En aquest sentit, l'Ajuntament disposa d'un mecanisme d'historials dels arxius. Aquest mecanisme indica qui ha realitzat accions sobre els arxius i quines accions s'han realitzat. L'Ajuntament establirà responsabilitats internes pel que fa a l'ús de la informació segons les persones que les han utilitzat. El sistema permet la generació dels informes corresponents.

5.9.5. Mesures que evitin pèrdues

L'Ajuntament disposa de mesures que eviten les pèrdues de la informació emmagatzemada. Qualsevol persona usuària no podrà esborrar la informació de l'Ajuntament. De la mateixa manera, qualsevol persona usuària, des de la seva carpeta sincronitzada no podrà modificar l'estructura d'arxius i carpetes de l'Ajuntament.

Mitjançant els permisos d'accés, es garantirà que cada persona usuària només accedeixi a la parcel·la d'informació composta per arxius i carpetes que ha d'utilitzar. Es concediran permisos per serveis, ningú ha d'accedir a carpetes que no siguin del seu servei o àmbit de gestió.

L'Ajuntament disposa d'un mecanisme de recuperació dels arxius o carpetes esborrats pel personal. Aquest mecanisme es concreta en una Paperera de Reciclatge, l'esborrat definitiu de la qual només podrà realitzar-se per una persona responsable del sistema, concretament l'Administrador.

L'Ajuntament també disposa de mecanismes de recuperació d'un fitxer modificat. En aquest sentit, té la possibilitat de recuperar la versió anterior d'un arxiu quan algun tipus d'error hagi fet que la versió actual ja no sigui vàlida.

5.9.6. Control d'enllaços i de correus electrònics enviats

El personal de l'Ajuntament haurà de tenir molta cura amb els enllaços per compartir arxius. En aquest sentit, els sistemes que utilitza permeten un control de l'accés a aquests enllaços. Per tal de controlar-los i el seu possible destí, l'Ajuntament disposa d'un control dels accessos als enllaços enviats.

Els enllaços tindran un temps de vida, bé limitat pel nombre d'accessos o per una caducitat. Els sistemes que permeten la generació d'enllaços sense control i de lliure accés no seran permesos per l'Ajuntament (per posar un exemple, si s'envia un contracte a un/a client/a mitjançant un enllaç no es pot permetre el lliure accés a aquest enllaç, ja que si algú copia i enganxa aquest enllaç a Facebook, milers de persones podrien descarregar el contracte).

5.9.7. Control de l'empresa propietària del servei de núvol

L'Ajuntament ha comprovat que qui proveeix el servei del núvol és una empresa amb una localització física comprovable.

L'Ajuntament comprovarà periòdicament, mitjançant contacte per email, si el proveïdor atén els seus clients i es tracta d'una empresa real i que està viva.

L'Ajuntament haurà de comprovar que l'empresa proveïdora declari públicament on emmagatzema les dades, això li permetrà comprovar per la web si el lloc d'emmagatzematge compta amb certificacions de seguretat i mesures de protecció de les dades.

5.10. Accés a internet

5.10.1. L'ús del sistema informàtic de l'Ajuntament per accedir a Internet es limitarà a les qüestions relacionades directament amb les funcions derivades de l'activitat desenvolupada a l'Ajuntament.

5.10.2. L'Ajuntament protegeix l'accés a internet mitjançant sistemes de control de navegació web, i aplicacions. Queda prohibit l'accés a aquelles pàgines que vulnerin les regles de navegació establertes a l'entitat. Qualsevol usuari que requereixi l'accés a alguna pàgina amb

accés restringit haurà de sol·licitar-ho a Sistemes d'Informació mitjançant un procediment CIM.INF.

5.10.3. No està permès l'intent d'evadir els filtres de navegació implementats per l'organització.

5.10.4. L'Ajuntament manté un registre d'accessos a internet. En el cas que es detectin indicis fonamentats d'un ús inadequat de l'accés a internet, com ara la reducció en la velocitat de la connexió a internet, l'Ajuntament podrà dur a terme un seguiment de l'adequada utilització d'aquests recursos per part de les persones usuàries.

5.11. Instal·lació i configuració dels equipaments informàtics

5.11.1. La instal·lació i/o configuració de maquinari és competència del personal del Servei de Tecnologies i Sistemes d'Informació designat per l'Ajuntament.

5.11.2. Les persones usuàries no poden modificar la configuració dels equips assignats. Qualsevol modificació en la configuració dels accessos a la xarxa haurà de ser realitzada pel personal del Servei de Tecnologies i Sistemes d'Informació.

5.11.3. De les configuracions i accessos a la xarxa o del correu electrònic de l'Ajuntament mitjançant dispositius que siguin propietat de l'usuari, se'n podrà donar compte periòdicament a la Comissió de Seguretat.

5.12. Gestió de llicències de programari

5.12.1. El Servei de Tecnologies i Sistemes d'Informació vetllarà per la coordinació de l'ús correcte de les llicències.

5.12.2. Així mateix, es promourà l'increment de l'ús d'eines de programari lliure.

5.13. Incidents de seguretat

S'entén per incident de seguretat, qualsevol anomalia que afecti o pugui afectar la seguretat de les dades, per exemple, la pèrdua de dades de forma accidental, el robatori d'expedients, la sospita d'intrusió a la xarxa corporativa, el deteriorament de suports de còpies de seguretat, correus electrònics sospitosos, virus, sospita de suplantació d'identitat corporativa en xarxes socials, robatori de contrasenyes, detecció de comportament anormal dels equips informàtics, pèrdua o robatori d'equips que contenen dades de propietat de l'Ajuntament, etc.

5.13.1. És obligació de totes les persones usuàries comunicar qualsevol incidència que es detecti durant el tractament de dades personals a les quals tinguin accés. Les incidències seran comunicades al Servei de Tecnologies i Sistemes d'Informació mitjançant el procediment de comunicació d'incidències. En la notificació, la persona usuària haurà de descriure la incidència que hagi detectat, especificant el tipus de suports afectats (documentació i/o fitxers informàtics).

5.13.2. La comunicació d'incidències de seguretat de dades s'haurà de realitzar en un termini no superior a una hora des de la seva detecció

mitjançant el procediment CIM.INF, tant per incidències en suport paper com en suport electrònic.

5.13.3. En cas de pèrdua o robatori d'equip informàtic que comprometi les dades de propietat de l'Ajuntament, s'enregistrarà en un procediment de seguretat SGI.PMI que posarà en coneixement automàtic a la Comissió de Seguretat.

5.13.4. Es donarà compte de les incidències de seguretat a la Comissió de Seguretat.

5.14. Protecció de dades

5.14.1. Per crear noves activitats de tractament de dades personals caldrà posar-ho en coneixement del Delegat o Delegada de Protecció de Dades, per tal que valori la sol·licitud i l'Ajuntament doni l'autorització, si correspon.

5.14.2. S'utilitzarà el procediment PDP.RAT per fer aquest tipus de sol·licituds.

5.15. Tractament d'informació temporal

S'entén per informació temporal aquella que es crea com a suport intermedi, en forma de fitxers, bases de dades o altres, necessària per elaborar una documentació o informació definitiva

5.15.1. Es poden crear fitxers temporals a partir de les bases de dades i documentació existents a l'Ajuntament.

5.15.2. La informació temporal haurà de mantenir les normes de seguretat de la mateixa manera que es mantenen per a la informació original.

5.15.3. Una informació temporal mantindrà la mateixa finalitat amb la qual va ser definida originalment.

5.15.4. Un cop finalitzada la vida útil de la informació temporal haurà de ser eliminada.

5.16. Tractaments en suports digitals i en suport paper

5.16.1. La documentació utilitzada per cada persona usuària per raó de la seva funció és propietat de l'Ajuntament.

5.16.2. Només es podrà accedir a la documentació del mateix àmbit en el qual es desenvolupi l'activitat.

5.16.3. La persona usuària és la responsable de la custòdia i la confidencialitat de la documentació que contingui dades de caràcter personal mentre en faci ús.

5.16.4. És d'obligat compliment vetllar que els documents tractats no es destrueixin o es deteriorin.

5.16.5. No està permesa la divulgació de documents que continguin dades de caràcter personal sense l'autorització de la Comissió de Seguretat.

5.17. Destrucció de documentació i els seus suports

5.17.1. Un cop acabada la vigència legal i les necessitats de tractament de la informació per part de l'Ajuntament, els suports que continguin dades de caràcter personal hauran de ser destruïts de forma controlada.

5.17.2. Per a la destrucció de documentació sigui en paper o digital els diferents serveis han d'utilitzar el procediment ARX.SED, que garanteix el compliment de la legislació vigent en matèria de destrucció de dades.

5.17.3. Quan es tracta de destrucció d'elements que formen part del Centre de Procés de Dades (CPD), la sol·licitud de destrucció es farà mitjançant el procediment ARX.SED.

5.17.4. La Comissió de Seguretat forma part d'aquest procediment.

5.18. Utilització dels dispositius portàtils corporatius (telèfons mòbils, tauletes, portàtils)

5.18.1. L'Ajuntament assignarà dispositius portàtils corporatius a aquelles persones usuàries que ho precisin per al desenvolupament de les seves funcions.

5.18.2. La configuració d'aquests dispositius serà realitzada per personal del Servei de Tecnologies i Sistemes d'Informació, establint un sistema de bloqueig del dispositiu que la persona usuària podrà personalitzar, però que en tot cas haurà de mantenir actiu.

5.18.3. No està permesa la descàrrega o instal·lació als dispositius portàtils propietat de l'Ajuntament, aplicacions (APP) que no tinguin relació directa amb les funcions desenvolupades a l'Ajuntament.

5.18.4. La utilització d'aquests dispositius que permetin la connectivitat per trucades i consum de dades mòbils es limitarà a allò que tingui relació amb les tasques relacionades amb les funcions de la persona usuària. L'Ajuntament es reserva el dret a portar a terme aquelles accions de control que siguin necessàries per garantir-ne un bon ús.

5.18.5. Com a norma general, no es podrà utilitzar la itinerància (roaming) fora de l'àmbit estatal. Si una persona usuària necessita tenir activada la itinerància, ho haurà de demanar a la Secció de Xarxes i Eficiència Energètica, amb la prèvia autorització del/de la respectiu/iva cap de servei.

5.18.6. La petició d'aquests tipus de dispositiu (tauletes o equips portàtils) es farà mitjançant el procediment de seguretat de préstec de material informàtic SGI.PMI)

5.19. Comunicació

5.19.1. Les persones que entrin a prestar servei a l'Ajuntament, amb caràcter temporal o indefinit, se'ls facilitarà l'accés a aquest document. A tots els efectes, la persona usuària acusarà l'accés al citat document.

5.19.2. Sempre que es produeixin modificacions del present Reglament es remetrà una circular informativa en la qual es farà referència a les possibles modificacions produïdes en aquest el document.

5.19.3. Altres accions de comunicació i de conscienciació previstes periòdicament són:

5.19.3.1. Sessions internes de presentació als equips de treball de les diferents àrees funcionals dels aspectes tècnics/metodològics de seguretat destacats.

5.19.3.2. Reunions periòdiques per tractar les qüestions que siguin d'interès general o particular per perfils (formació, canvis organitzatius, procés de seguretat i avaluació del grau de compliment, etc.).

5.19.4. En aquestes accions, participen totes les persones professionals de les diverses àrees, o una part en els casos que l'activitat hagi estat encaminada a un perfil concret, raó per la qual han de ser coordinades pels/per les responsables de les àrees.

5.20. Responsabilitat

El compliment de les responsabilitats associades a la custòdia de les dades de l'Ajuntament i la protecció del sistema d'informació tenen caràcter obligatori.

5.20.1. L'incompliment per part de les persones usuàries de l'Ajuntament de les obligacions contingudes en el present Reglament serà sancionat disciplinàriament, tenint en compte la gravetat de l'incompliment i d'acord amb la normativa corresponent.

5.20.2. Les responsabilitats civils o penals que es derivin de les actuacions infractores de les persones usuàries seran exigides de conformitat amb la legislació vigent.

5.20.3. En el cas de personal extern a l'Ajuntament, el seu incompliment pot implicar l'exigència de responsabilitats civils o penals, a banda de la reclamació d'indemnització per danys i perjudicis ocasionats, així com les derivades de l'incompliment de l'obligació contractual.

5.20.4. Si els fets suposessin la imputació d'una infracció a l'ús inadequat de les dades de caràcter personal, l'Autoritat Catalana de Protecció de dades, a través de l'òrgan sancionador corresponent, podria proposar la iniciació d'actuacions disciplinàries.

5.20.5. Qualsevol actuació que contradigui o no estigui especificada en els punts d'aquest reglament, haurà de ser revisada per la Comissió de Seguretat de l'Ajuntament de Manresa que en donarà el curs oportú.

6. Recomanacions i bones pràctiques

6.1. S'ha d'utilitzar el sistema de bloqueig de terminal, en cas d'absència temporal del lloc de treball (prement simultàniament, les tecles de l'ordinador

Alt+Ctrl+Supr). Quan vulguem recuperar la sessió, caldrà prémer la mateixa seqüència de tecles, i introduir la contrasenya de la xarxa.

6.2. Evitar mantenir obertes aplicacions o navegadors si no s'estan fent servir, sobretot quan es finalitza la jornada laboral.

6.3. Per tal de millorar l'eficiència del nostre Ajuntament a efectes d'estalvis econòmics i de benefici del medi ambient, cal l'acompliment de les següents recomanacions:

6.3.1. Apagueu el PC i la impressora cada dia en sortir de la feina per tal d'estalviar energia.

6.3.2. Compartiu els dispositius informàtics sempre que sigui possible i d'acord amb els/les responsables del servei al qual pertanyeu. Estalviareu consumibles, trànsit d'informació a la xarxa, costos de manteniment, etc.

6.3.3. Feu impressions només si és imprescindible i, sempre que sigui possible, utilitzant l'opció de doble cara.

6.3.4. Eviteu al màxim possible la impressió en color.

6.3.5. Manteniu ocupat el mínim espai en disc necessari, reviseu periòdicament l'organització de les carpetes i els documents. No guardeu documents sense una causa justificada.

6.3.6. Utilitzeu les carpetes compartides per la informació que ha de ser accessible per diverses persones.

6.3.7. Ús dels equips de telefonia només quan sigui necessari i només per a comunicacions relacionades amb el lloc de treball. En aquest sentit, l'Ajuntament portarà un control exhaustiu dels costos telefònics de cada telèfon fix o mòbil.

6.3.8. Ús dels serveis d'internet i de les xarxes socials només quan sigui necessari i per a tasques relacionades amb el lloc de treball. L'Ajuntament portarà un control dels llocs i el temps que des de cada PC es navega per internet.

6.3.9. Es recomana activar el doble factor d'autenticació a totes les aplicacions en què hi hagi la disponibilitat per fer-ho.

7. Disposició transitòria

A causa de la seva variabilitat i constant dinàmica evolutiva, totes aquelles especificacions tècniques, aplicacions, dispositius tecnològics o procediments que apareixen en aquest reglament, si no alteren el sentit general de l'article en què figuren, seran susceptibles de modificació mitjançant resolució.

8. Disposició derogatòria

Queda derogat el Reglament d'ús de les dades personals i els sistemes d'informació de l'Ajuntament de Manresa, aprovat inicialment per acord de ple de 24 de setembre de 2020,

aprovació que esdevingué definitiva en no haver-s'hi presentat al·legacions (BOP de 9 de desembre de 2020).

9. Disposicions finals

Primera

Aquest codi ha estat tramitat per l'òrgan competent i es mantindrà vigent mentre no se n'aprovi expressament la seva modificació o derogació. El present Reglament s'haurà de revisar i actualitzar periòdicament, d'acord amb l'evolució dels mitjans tècnics i organitzatius, seguint el procediment administratiu previst per a la seva aprovació.

Segona

Aquest Reglament entrarà en vigor un cop sigui aprovat definitivament, se n'hagi publicat el text íntegre al Butlletí Oficial de la Província de Barcelona i hagi transcorregut el termini previst als articles 65.2 i 70.2 de la Llei 7/1985, de 2 d'abril, reguladora de les bases de règim local.

Marc Aloy Guàrdia.
L'alcalde,

Signat electrònicament
per: MARC ALOY
GUARDIA
Data: 20/05/2024
11:34:37
Raó: Signatura
Lloc: Manresa