Ajuntament d'Arenys de Munt

Política de Seguretat de la Informació

Exp.1820/2023

VERSIÓ	DATA	CANVIS REALITZATS	RESPONSABLE
1.0	Febrer de 2023	DOCUMENT INICIAL	Ajuntament d'Arenys de Munt

Índex de continguts ..... ***Error! No s'ha definit el marcador.***

1. Introducció *3*

1.1 Abast 4

1.2 Missió 4

1.3 Aprovació i entrada en vigor 4

2. Marc legislatiu *5*

3. Principis de compliment de la política de seguretat *6*

3.1 Dades de caràcter personal 6

3.2 Gestió de riscos 7

3.3 Prevenció i reacció davant incidències 7

4. Organització de la seguretat *9*

4.1 Funcions i responsabilitats 9

4.1.1 Responsable de la Informació 10

4.1.2 Responsable de Seguretat 10

4.1.3 Responsable del Sistema 11

4.1.4 Responsables de Serveis 12

4.2 Procediments de designació 12

5. Obligacions del personal *13*

6. Terceres parts *14*

7. Gestió i desenvolupament de la política de seguretat de la informació *15*

7.1 Revisió de la política de seguretat de la informació 15

1. Introducció

L'Ajuntament d'Arenys de Munt, d'ara endavant l'Ajuntament, en tant que com Administració Pública al servei de la ciutadania disposa d'una infraestructura de Tecnologies d'Informació i Comunicacions (TIC) per a desenvolupar les seves competències i assolir els seus objectius.

La gestió de les TIC ha de ser portada a terme aplicant les mesures necessàries que li permetin garantir la protecció davant de les possibles incidències (accidentals o deliberades) que es puguin produir, de forma que es puguin minimitzar les afectacions sobre la disponibilitat, integritat o confidencialitat de la informació relacionada amb els serveis prestats.

La qualitat de la informació i la prestació continuada de serveis hauran de ser garantits actuant de forma preventiva, mitjançant una adecuada supervisió periòdica i constant, tenint com a objectiu final la seguretat de la informació com a cultura general a l'entitat.

D'acord amb allò que s'estableix a l'article 12.6 del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), la política de seguretat s'ha d'establir sobre la base dels principis bàsics en l'àmbit de l'Administració electrònica i estableix que tots els òrgans superiors de les administracions públiques han de disposar formalment de la seva política de seguretat, i s'ha de desenvolupar aplicant els requisits mínims següents en proporció als riscos identificats en cada sistema:

a) Organització i implantació del procés de seguretat.

b) Anàlisi i gestió dels riscos.

c) Gestió de personal.

d) Professionalitat.

e) Autorització i control dels accessos.

f) Protecció de les instal·lacions.

g) Adquisició de productes de seguretat i contractació de serveis de seguretat.

h) Mínim privilegi.

i) Integritat i actualització del sistema.

j) Protecció de la informació emmagatzemada i en trànsit.

k) Prevenció davant d'altres sistemes d'informació interconnectats.

l) Registre de l'activitat i detecció de codi nociu.

m) Incidents de seguretat.

n) Continuïtat de l'activitat.

o) Millora contínua del procés de seguretat.

Així mateix, l'article 12.2 de l'ENS indica que la política de seguretat ha de ser formalment aprovada per l'òrgan competent

Per tot el que s'exposa anteriorment, en aquest document es defineix la política de seguretat de la informació de l'Ajuntament.

1.1 Abast

Aquesta política s'aplica a tots els sistemes TIC (infraestructures, programari, comunicacions,...) de l'Ajuntament i a tots els seus membres, sense excepcions.

1.2 Missió

Mitjançant la present Política de Seguretat l'Ajuntament d'Arenys de Munt expressa el seu compromís amb l'administració de la seguretat de la seva informació, d'acord amb els requeriments propis, així com amb les lleis i normatives vigents.

1.3 Aprovació i entrada en vigor

Aquesta política de seguretat de la Informació és efectiva des de la data d'aprovació mitjançant Decret d'Alcaldia i fins que sigui reemplaçada per una nova política.

2. Marc legislatiu

L'ús de les TIC per part de l'Ajuntament d'Arenys de Munt es troba regulat per les següents normes jurídiques:

ESTATAL

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Reial decret 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat.
- Reial decret 4/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional d'Interoperabilitat.
- Reglament (UE) 2016/679 del Parlament 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 (RGPD).
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD)
- Reial decret 1671/2009, de 6 de novembre, pel que es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.
- Llei 6/2020, de 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança
- Reial Decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics
- Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic.
- Instruccions del Centre Criptogràfic Nacional, CCN-STIC.

AUTONÒMICA

- Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya.
- Llei 29/2010, de 3 d'agost, d'ús dels mitjans electrònics al sector públic de Catalunya.

LOCAL

- Ordenança reguladora de l'Administració Electrònica a l'Ajuntament.
- Reglament Orgànic Municipal (ROM).

3. Principis de compliment de la política de seguretat

Les TIC utilitzades per l'Ajuntament han de disposar d'elements que en garanteixin una protecció adient contra amenaces que, degut a la seva constant evolució, tenen un gran potencial per a produir afectacions en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els serveis.

Amb l'objectiu de disposar d'elements per a la defensa d'aquestes amenaces, l'Ajuntament necessita disposar d'una estratègia que s'adapti als canvis constants que es produeixen a l'entorn per garantir la prestació contínua dels serveis. Això implica que l'Ajuntament ha d'aplicar les mesures mínimes de seguretat exigides pel Reial decret 311/2022, de 3 de maig, que regula l'ENS, així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

L'Ajuntament ha de garantir que la seguretat TIC esdevingui un element integral del sistema, des del seu disseny inicial fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició de programari i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació de l'àrea, en la sol·licitud de propostes de serveis, i en la elaboració dels plecs per a la licitació de projectes relacionats amb les TIC.

Els procediments i normatives aplicables als sistemes informàtics i organització informàtica es recull als Procediment tècnics TIC.

3.1 Dades de caràcter personal

L'Ajuntament, en el desenvolupament de les seves competències. tracta dades personals de la ciutadania, del seu personal i de tercers.

Els sistemes d'informació que tractin dades personals hauran d'aplicar el que disposa la normativa vigent en matèria de protecció de dades personals. Per a això, l'Ajuntament amb l'assessorament i participació del Delegat de Protecció de Dades realitzarà una anàlisi de riscos d'acord el definit als articles 24 i 32 de l'RGPD i, si s'escau, una avaluació d'impacte en la protecció de dades dels tractaments de l'Ajuntament.

Els sistemes d'informació de l'Ajuntament han d'aplicar les mesures de seguretat resultants d'aquests anàlisis, que prevaldran si són més exigents a les definides per l'Esquema Nacional de Seguretat.

3.2 Gestió de riscos

Tots els sistemes subjectes a aquesta política hauran de ser objecte d'un anàlisi de riscos, on s'avaluïn les amenaces i els riscos a què estan exposats.

Aquesta anàlisi es portarà quan es produeixin les següents circumstàncies:

- Regularment, almenys un cop l'any.
- Quan es produeixin canvis en la informació tractada.
- Quan es produeixin canvis en els serveis prestats.
- Quan es detecti una incidència de seguretat greu.
- Quan es detectin vulnerabilitats greus.

Per a l'harmonització dels anàlisis de riscos, l'Ajuntament establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats.

L'Ajuntament garantirà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

3.3 Prevenció i reacció davant incidències

El personal de l'Ajuntament ha de disposar dels mecanismes per a la prevenció, detecció, resposta i conservació per a minimitzar les vulnerabilitats, evitar que les amenaces es materialitzin i – en cas contrari - reaccionar davant de possibles incidents, d'acord amb l'article 8 i 25 de l'ENS, i l'article 33 de l'RGPD si afecta dades personals.

La seguretat del sistema ha de contemplar les accions relatives als aspectes de prevenció, detecció i resposta, a fi de minimitzar les seves vulnerabilitats i aconseguir que les amenaces sobre aquest no es materialitzin o que, en el cas de fer-ho, no afectin greument la informació que maneja o als serveis que presta.

Les mesures de prevenció, que poden incorporar components orientats a la dissuasió oa la reducció de la superfície d'exposició, han d'eliminar o reduir la possibilitat que les amenaces arribin a materialitzar-se.

Les mesures de detecció aniran dirigides a descobrir la presència d'un incident de seguretat.

Les mesures de resposta, que es gestionaran en temps oportú, estaran orientades a la restauració de la informació i els serveis que es puguin haver vist afectats per un incident de seguretat.

El sistema d'informació garantirà la conservació de les dades i informació en suport electrònic, garantint que la seva aplicació no suposi una reducció en l'aplicació principis bàsics i requisits mínims establerts,.

De la mateixa manera, el sistema mantindrà disponibles els serveis durant tot el cicle vital de la informació digital, mitjançant una concepció i procediments que siguin la base per a la preservació del patrimoni digital.

4. Organització de la seguretat

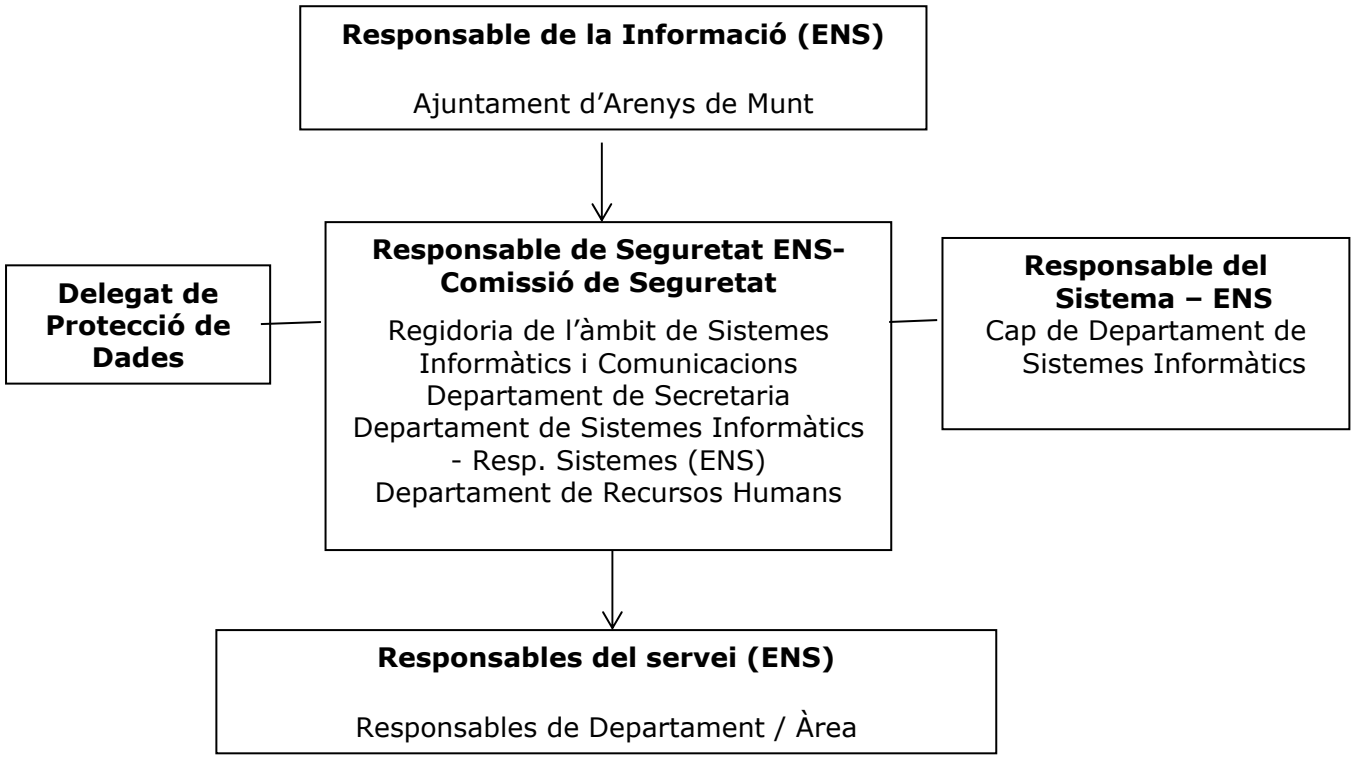
4.1 Funcions i responsabilitats

Els rols i les funcions de l'organització de la seguretat establerts a l'Esquema Nacional de Seguretat seran assumits per la Comissió de Seguretat i el rol de Responsable del Sistema que serà assumit per la Cap de Departament de Sistemes i Tecnologies de la Informació.

Les Responsabilitats dels Òrgans de Direcció de l'Ajuntament d'Arenys de Munt respecte al compliment de la legislació són:

- Assignar al ***Comissió de Seguretat*** a càrrec de coordinar i controlar les mesures definides en a la present Política de Seguretat.
- Nomenar el **Responsable de Seguretat**, tasca assumida per la ***Comissió de Seguretat***.
- Donar el suport i dotar dels recursos necessaris al ***Comissió de Seguretat*** i a la ***Cap de Departament de Sistemes i Tecnologies de la Informació*** per a poder portar a terme les seves funcions.

La Organització per a la gestió de la protecció de dades de l'Ajuntament d'Arenys de Munt és:



4.1.1 Responsable de la Informació

Responsable de la Informació	Alcaldia
Funcions	1. Nomenar el Responsable de Seguretat ENS, tasca assumida per la Comissió de Seguretat. 2. Nomenar el Responsable del Sistema, tasca assumida per la Cap de Departament de Sistemes i Tecnologies de la Informació 3. Donar el suport i dotar dels recursos necessaris al Responsable de Seguretat i al Responsable del Sistema per a poder portar a terme les seves funcions.

4.1.2 Responsable de Seguretat

Responsable de Seguretat	Comissió de Seguretat
Composició	• Alcalde / Regidoria de l'àmbit TIC • Secretaria • Cap de Departament de Sistemes i Tecnologies de la Informació - Resp. Sistemes (ENS) • Cap del Departament de RH
Funcionament	• 1 reunió semestral, amb caràcter ordinari • Extraordinàriament, aquesta Comissió es reuniria per tractar temes urgents i/o de necessitat.
Actua com a secretari/a	Secretaria amb la col·laboració de personal administratiu en qui es delegui, que exercirà les següents funcions: • *Coordinar i preparar l'agenda de les reunions i enviar comunicacions de convocatòries.* • *Elaborar actes de les reunions ordinàries i extraordinàries* • *Gestió administrativa de la documentació emesa per la Comissió.* • *Comunicació al personal i responsables de les decisions preses pel Comissió de Seguretat.*
Relació amb la les dades personals	La Comissió de Seguretat implanta les mesures per a la protecció de les dades i dona suport al DPD
Funcions	• Establir, impulsar i garantir l'aplicació i el compliment de les polítiques i procediments de Seguretat aprovats per l'Ajuntament. • Validar i tramitar l'aprovació de la documentació relacionada amb la seguretat de la informació (Política de Seguretat, Reglaments Interns,...).

	• Garantir la correcta implantació de les polítiques i procediments de Seguretat. • Promoure les auditories i controls regulars que permetin verificar el compliment de les obligacions de l'Ajuntament en seguretat de la informació. • Promoure la formació i conscienciació de la seguretat de la informació al personal de l'Ajuntament. • Garantir, amb el suport del Responsable del Sistema, la implantació i control de les mesures de seguretat de manera que aquestes s'integrin adequadament a l'operativa d'Administració Electrònica. • Garantir la correcta regulació legal dels proveïdors de tecnologies d'informació que suportin els serveis vinculats a l'ENS. • Vetllar per tal que es dugui a terme el preceptiu procés d'anàlisi i gestió de riscos en el sistema. • Fer el seguiment dels incidents de seguretat que hagin ocorregut relatius a la seguretat de la informació, amb el suport del Responsable del Sistema.

4.1.3 Responsable del Sistema

Responsable del Sistema	Cap de Departament de Sistemes Informàtics
Funcions delegades	1. Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar el seu correcte funcionament i operativitat. 2. Gestió, configuració i actualització, del maquinari i programari sota el seu àmbit de gestió en què es basen els mecanismes i serveis de seguretat del sistema. 3. Implementació, gestió i manteniment de les mesures de seguretat aplicables al sistema que es trobi sota el seu àmbit de gestió. 4. Interlocució amb dels proveïdors de tecnologies d'informació que suportin els serveis vinculats a l'ENS. 5. Assegurar que la traçabilitat, auditoria i altres registres de seguretat es duen a terme sovint, d'acord amb la política de seguretat establerta. 6. Establir procediments de seguiment i reacció davant incidències. 7. Donar d'alta nous rols d'accés als programes i aplicacions corporatives que es trobin sota el seu àmbit de gestió.

4.1.4 Responsables de Serveis

Responsables de Serveis	Responsables de Departament / Àrea
Funcions delegades	1. Definir els serveis necessaris per portar a terme les competències de l'Ajuntament d'Arenys de Munt. 2. Vetllar pel compliment de les polítiques i normes de seguretat determinades per l'Ajuntament d'Arenys de Munt en la gestió dels serveis i en el tractament de la informació de l'àmbit de responsabilitat. 3. Implementar totes les mesures de seguretat definides a la documentació de seguretat per a sistemes d'informació no automatitzats (arxiu i emmagatzematge de documentació). 4. Definir els perfils i criteris d'accés a la documentació i aplicacions informàtiques sota l'àmbit de àmbit de responsabilitat. 5. Concedir o denegar l'autorització d'accés als usuaris a la informació sota el seu àmbit de responsabilitat.

4.2 Procediments de designació

El responsable de Seguretat i el Responsable de Sistema, així com la comissió, seran nomenats per Decret d'Alcaldia. El nomenament s'ha de revisar cada 2 anys o quan el lloc quedi vacant.

En el cas de que un Departament responsable presti electrònicament un servei sense la gestió ni coordinació o com a mínim la comunicació prèvia a la Comissió de Seguretat i – si s'escau Departament de Sistemes - haurà de designar el Responsable del Sistema i el Responsable de Seguretat que hauran de ser aprovats per Alcaldia, precisant les seves funcions i responsabilitats dins el marc establert per aquesta Política, d'acord a la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans al serveis públics i sota la seva directa responsabilitat.

5. Obligacions del personal

Tots els membres de l'Ajuntament tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, i el Responsable de Seguretat disposarà dels mitjans necessaris perquè la informació arribi als afectats.

Tots els membres de l'Ajuntament atendran a una sessió de conscienciació en matèria de seguretat TIC quan el Responsable de Seguretat ho estimi necessari. Igualment s'establirà un programa de conscienciació contínua per atendre tots els membres de l'Ajuntament, en particular als de nova incorporació.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al maneig segur dels sistemes en la mesura que la necessitin per realitzar-la. La formació és obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

Les obligacions del personal es troben recollides a Normativa interna d'ús dels sistemes d'informació i dades personals. aprovada per decret 360/2023, que s'acompanya al present document. (Annex Decret).

6. Tercers

Quan l'Ajuntament presti serveis a altres organismes o gestioni informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, s'establiran canals per informe i coordinació dels respectius Responsables de Seguretat i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan l'Ajuntament utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta política de seguretat i de la normativa de seguretat que pertoqui a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, i poden desenvolupar els seus propis procediments operatius per satisfer-la. S'establiran procediments específics d'informe i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta política.

Quan algun aspecte de la política no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precisi els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant.

Aquestes obligacions seran regulades mitjançant acord, conveni o contracte que defineixi la relació amb els tercers així com els criteris de nivell de servei i els sistemes de control i monitorització del compliment.

7. Gestió i desenvolupament de la política de seguretat de la informació

Aquesta política s'ha de desenvolupar per mitjà de normativa de seguretat que afronti aspectes específics. La normativa de seguretat estarà a disposició de tots els membres de l'organització que necessitin conèixer-la, en particular per aquells que utilitzin, operin o administrin els sistemes d'informació i comunicacions.

La normativa de seguretat estarà disponible a la Unitat de servidor definida per als documents a compartir entre el personal de l'Ajuntament.

La política serà aprovada per Decret d'Alcaldia, i difosa perquè la coneguin totes les parts afectades.

7.1 Revisió de la política de seguretat de la informació

Per verificar que s'acompleix amb tot allò que queda establert en aquesta Política de Seguretat, es realitzaran els controls interns que determini el Responsable de Seguretat (la Comissió de Seguretat), en el referent als sistemes d'informació.

La periodicitat d'aquests controls serà definida per la Comissió de Seguretat, existint també la possibilitat de portar a terme altres controls que pugui determinar en funció del desenvolupament de les operacions.

L'objectiu de les auditories serà el de verificar la possibilitat que els controls establerts a través de les mesures de seguretat siguin efectius; i que sigui possible garantir la integritat, la confidencialitat i la disponibilitat de la informació, les dades personals i els serveis TIC.

Serà missió del Responsable de Seguretat la revisió anual d'aquesta Política de Seguretat de la Informació i la proposta de revisió o manteniment de la mateixa. La política serà aprovada per Decret d'Alcaldia i difosa perquè la coneguin totes les parts afectades.

Ajuntament
d'Arenys de Munt

Normativa interna d'ús dels sistemes d'informació i dades personals

Ajuntament
d'Arenys de Munt

1. Funcions i Obligacions de les persones usuàries 3
2. Glosari 3
3. Àmbit d'aplicació 4
4. Obligacions de les persones usuàries 4
4.1 Obligacions generals respecte a la utilització dels Sistemes d'Informació 5
4.2 Gestió de peticions al Departament de Sistemes Informàtics 5
4.3 Deure de Confidencialitat 5
4.4 Utilització de credencials (usuari i contrasenya) i certificats digitals 6
4.5 Utilització de la xarxa corporativa 7
4.6 Enviaments de dades per mitjans telemàtics 8
4.7 Dispositius d'impressió 8
4.8 Treball fora de les dependències de l'Ajuntament 8
4.9 Utilització de dispositius externs 9
4.10 Ús del correu electrònic 9
4.11 Accés a Internet 10
4.12 Instal·lació i configuració dels equipaments informàtics 11
4.13 Propietat intel·lectual i industrial 11
4.14 Incidents de seguretat 11
4.15 Protecció de dades 12
4.16 Tractaments temporals 12
4.17 Tractaments en suports no automatitzats (documentació paper) 12
4.18 Destrucció de suports 13
4.19 Utilització dels dispositius portàtils corporatius (telèfons mòbils, tauletes) 13
5 Comunicació 14
6 Responsabilitat 14

1. FUNCIONS I OBLIGACIONS DE LES PERSONES USUÀRIES

Amb l'objectiu de garantir un ús adient de les dades de caràcter personal i dels sistemes d'informació a l'Ajuntament d'Arenys de Munt (d'ara endavant l'Ajuntament) defineix la present Normativa Interna d'ús dels sistemes d'informació i dades personals.

2. GLOSARI

• **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.

• **Persones usuàries**: Son les persones que es relacionen a l'article 3 de la present normativa.

• **Comissió de Seguretat:** Serà un òrgan col·legiat format pel Departament de Secretaria, Departament de Recursos Humans i el Departament de Sistemes Informàtics, que es crearà pròximament i que s'encarregarà de definir aquells protocols i mesures per tal de garantir la seguretat de la informació. El mecanisme de comunicació amb la Comissió serà l'adreça de correu electrònic comissioseguretat@arenysdemunt.cat.

• **Departament de Sistemes Informàtics**: És el Departament de l'Ajuntament que s'encarrega de la gestió dels Sistemes d'Informació corporatius, sent el responsable de tramitar totes les sol·licituds relacionades amb aquests.

• **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 composats d'un número identificador i contrasenya, o certificat digital.

• **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).

• **Xarxa corporativa**: Conjunt de carpetes compartides entre les persones usuàries d'un Departament o entre diferents Departaments de l'Ajuntament, on les persones usuàries

hi emmagatzemen els fitxers informàtics utilitzats per al desenvolupament de les funcions associades al lloc de treball.

• **Unitat C:** Unitat d'emmagatzematge local dels equips informàtics assignats, que no es troba connectada a la xarxa corporativa.

• **Enviament telemàtic**: Enviament de documents electrònics a tercers que no estigui relacionat amb notificacions electròniques o trameses a altres administracions públiques.

• **Núvol corporatiu:** És l'eina corporativa habilitada per l'Ajuntament per a la realització d'enviaments telemàtics a tercers.

3. ÀMBIT D'APLICACIÓ

La present Normativa Interna és d'aplicació a la totalitat de les persones usuàries dels sistemes d'informació de l'Ajuntament i accés a les dades confidencials i personals:

- Càrrecs electes
- Personal Funcionari, ja sigui interí o de carrera
- Personal Laboral, ja sigui temporal o fix
- Personal Eventual
- Personal Temporal
- Personal en pràctiques
- Personal d'empreses adjudicatàries
- Altres perfils que puguin accedir a dades de caràcter personal

4. OBLIGACIONS DE LES PERSONES USUÀRIES

4.1 OBLIGACIONS GENERALS RESPECTE A LA UTILITZACIÓ DELS SISTEMES D'INFORMACIÓ

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.

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.

3. Les tasques professionals s'hauran de realitzar de manera prioritària amb els equips informàtics corporatius, amb l'excepció de la realització de tasques en règim de teletreball que es troben autoritzades. Qualsevol excepció a aquesta situació haurà de ser corresponentment autoritzada per la Comissió de Seguretat.

4. Els equipaments informàtics assignats per al desenvolupament de tasques professionals hauran de ser retornats a l'Ajuntament un cop finalitzada la prestació de serveis

5. 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 realitzi un ús adequat d'acord al 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.

4.2 GESTIÓ DE PETICIONS AL DEPARTAMENT DE SISTEMES INFORMÀTICS

1. A efectes de garantir la traçabilitat de les tasques realitzades, totes les peticions al Departament de Sistemes Informàtics s'hauran de realitzar per escrit mitjançant l'adreça de correu electrònic informatica@ademunt.cat.

2. En cas que, degut a la naturalesa de la sol·licitud, no es pugui accedir al sistema informàtic caldrà connectar-se al correu electrònic mitjançant navegador per tal de trametre la sol·licitud.

4.3 DEURE DE CONFIDENCIALITAT

1. Les persones usuàries hauran de guardar, la màxima reserva i no divulgar ni utilitzar, directament ni a través de terceres persones o empreses, 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. Aquesta obligació continuarà vigent després de l'extinció de la seva relació amb el titular del fitxer o el seu responsable.

2. Està prohibit 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 excepció que es compti amb autorització expressa del Responsable del Tractament, que és l'Alcalde/essa.

3. En el cas que, per motius directament relacionats amb el lloc de treball, la persona usuària entri en possessió d'informació confidencial en qualsevol tipus de suport, s'haurà d'entendre que aquesta possessió és estrictament temporal, i sense que aquesta circumstància li atorgui cap dret de possessió o titularitat o còpia que cobri l'esmentada informació.

4. D'aquesta manera, la persona usuària 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 relació laboral.

4.4 UTILITZACIÓ DE CREDENCIALS (USUARI I CONTRASENYA) I CERTIFICATS DIGITALS

1. Les credencials assignades a una persona usuària són d'utilització exclusiva d'aquesta, quedant estrictament prohibit compartir-les amb qualsevol altra persona usuària. En cas d'incompliment d'aquesta prohibició, la persona usuària serà l'únic responsable dels actes realitzats amb el seu identificador.

2. Si la persona usuària necessita reiniciar la seva contrasenya d'accés a la xarxa corporativa ho haurà de tramitar la sol·licitud al Departament de Sistemes Informàtics enviant un correu electrònic a l'adreça de correu electrònic indicada a l'apartat 4.2, en cas que la sol·licitud de modificació de credencials vingui motivada per una sospita de suplantació haurà d'indicar-ho en el moment de tramitar la sol·licitud per tal que es procedeixi a realitzar les revisions pertinents.

3. La modificació de les credencials d'accés a aplicacions de tercers haurà de ser tramitada mitjançant el sistema habilitat per a aquest tercer.

4. El responsable jeràrquic de la persona usuària no podrà sol·licitar la utilització de les seves credencials a Informàtica. En cas que res rebi alguna petició d'aquest tipus aquesta serà remesa a la Comissió de Seguretat per a la seva valoració

4.5 UTILITZACIÓ DE LA XARXA CORPORATIVA

1. Les dades corporatives hauran de ser emmagatzemades a les unitats dels servidors corporatius assignades pel Departament de Sistemes Informàtics.

2. Les carpetes de la xarxa corporativa són organitzades d'acord a la següent tipologia:

• Unitats Departamentals: Destinades a l'emmagatzematge de la informació de cada Departament.

• Unitat Compartida: Destinada a compartir informació entre els diferents Departaments.

• Unitat Personal: Destinada a l'emmagatzematge d'informació personal relativa a la relació laboral amb l'Ajuntament (Sol·licituds a Recursos Humans,...).

3. Les unitats indicades anteriorment són per a l'emmagatzematge exclusiu d'informació relacionada amb l'activitat de l'Ajuntament. Queda expressament prohibida la introducció d'altre tipus de continguts en aquestes unitats.

4. En cas que es precisi el tractament d'imatges aquestes hauran de ser emmagatzemades a la unitat específica configurada pel Departament de Sistemes Informàtics.

5. La informació emmagatzemada a la unitat departamental haurà d'estar classificada d'acord als criteris de classificació definits i aprovats per l'Ajuntament d'acord a la normativa vigent, de forma que aquesta informació sigui de fàcil localització i d'acord a la utilitat de la mateixa per al Departament i el conjunt de l'Ajuntament.

6. Les unitats C de l'equip assignat no són en cap cas unitats d'emmagatzematge d'informació, l'Ajuntament no podrà garantir la recuperació de la informació emmagatzemada en cas d'incidència.

4.6 ENVIAMENTS DE DADES PER MITJANS TELEMÀTICS

1. 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 d'altres administracions públiques que es realitzaran mitjançant les plataformes habilitades i les notificacions electròniques.

2. Les transmissions de dades fora de la xarxa corporativa hauran de ser realitzades mitjançant el núvol corporatiu habilitat pel Departament de Sistemes Informàtics, queda prohibida qualsevol transmissió de dades de caràcter personal amb qualsevol altre tipus d'eina (correu electrònic o núvols de tercers).

3. Per a poder realitzar enviaments caldrà sol·licitar accés al núvol corporatiu al Departament de Sistemes Informàtics mitjançant el sistema de peticions.

4. Els enviaments d'informació s'hauran de realitzar mitjançant fitxer comprimit protegit amb contrasenya, la contrasenya s'enviarà a la persona destinatària en un missatge a banda per correu electrònic.

4.7 DISPOSITIUS D'IMPRESSIÓ

1. La utilització de dels dispositius d'impressió corporatius es limitarà a aquella documentació que sigui necessària per al desenvolupament de les funcions de la persona usuària.

2. En el cas que sigui necessari realitzar impressions caldrà aplicar les mesures necessàries per a garantir l'estalvi de recursos en funció de les característiques de cada dispositiu (impressions a doble cara, impressions amb escala de grisos,...).

3. Les persones usuàries hauran de garantir que no quedin documents impresos en la safata de sortida dels dispositius d'impressió.

4.8 TREBALL FORA DE LES DEPENDÈNCIES DE L'AJUNTAMENT

1. L'Ajuntament habilitarà accessos remots per al treball fora de les dependències de l'Ajuntament a aquelles persones usuàries o tercers que ho precisin per al

desenvolupament de les seves funcions, sempre s'autoritzi seguint els canals establerts al Reglament de Teletreball.

2. Els accessos remots als sistemes corporatius es realitzaran amb els equips particulars de cada persona usuària, sempre que s'acompleixin els requisits de seguretat establerts pel Departament de Sistemes Informàtics. En cas de no poder acomplir aquests requisits l'Ajuntament assignarà un equip a la persona usuària sempre que n'hi hagi disponibles.

4.9 UTILITZACIÓ DE DISPOSITIUS EXTERNS

1. Per defecte no es permet la utilització de dispositius d'emmagatzematge extern (dispositius de memòria USB o similars) per a la càrrega i la descàrrega de continguts de la Xarxa Corporativa.

2. En el cas que, per motius relacionats amb el lloc de treball, sigui necessari utilitzar aquest tipus de dispositius serà necessari comptar amb autorització de la Comissió de Seguretat.

3. En cas de comptar amb autorització caldrà utilitzar exclusivament els dispositius facilitats pel Departament de Sistemes Informàtics.

4.10 ÚS DEL CORREU ELECTRÒNIC

1. Es considerarà correu electrònic qualsevol adreça electrònica corporativa generada dins del domini de l'Ajuntament (@ademunt.cat, @arenysdemunt.cat).

2. L'Ajuntament assignarà un compte personal de correu electrònic personal per a la persona usuària en cas que ho necessiti per al desenvolupament de les seves funcions, aquest compte serà personal i intransferible.

3. Les adreces genèriques de cada Departament definides seran responsabilitat del seu Cap, sent aquest l'encarregat de definir la seva utilització. En tot cas aquests comptes no podran ser utilitzats com a bústia de correu electrònic de les persones usuàries.

4. En cas d'una absència programada (vacances, permisos,...) la persona usuària serà responsable de programar de una auto resposta al seu compte de correu electrònic informant d'aquesta situació. El text programat a l'auto resposta serà definit per la pròpia persona usuària, podent indicar una adreça de correu electrònic al qual les

persones es puguin dirigir. En cas que degut a l'absència no permeti configurar-ho ell mateix ho requerirà a Informàtica. En aquells casos que la persona usuària no ho hagi requerit la Comissió de Seguretat podrà determinar la necessitat d'activar-ho.

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.

6. No es podran descarregar fitxers des del compte de correu electrònic que no tinguin relació amb les tasques desenvolupades a l'Ajuntament. Concretament les persones usuàries hauran de vigilar, entre d'altres, amb aquells correus enviats per usuaris coneguts amb idioma estranger, correus amb fitxers adjunts que no hagin estat sol·licitats prèviament, correus amb un assumpte no definit.

7. En cas de rebre un correu de la tipologia descrita a l'apartat anterior o similar, o qualsevol tipus de correu sospitós caldrà informar-ne a Informàtica amb la màxima celeritat a l'adreça de correu electrònic.

8. 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 de difusió d'informació habilitats per l'Ajuntament.

9. En cas que una persona usuària causi baixa dins l'organització, es mantindrà durant un mes la seva bústia personal, en previsió de necessitats del servei al qual estava adscrit o per motius legals. Passat aquest termini la bústia serà inhabilitada.

4.11 ACCÉS A INTERNET

1. L'ús dels Sistemes d'Informació 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.

2. Queda prohibit l'accés a aquelles pàgines vulnerin les regles de navegació establertes a l'entitat com ara les plataformes de reproducció de vídeo, qualsevol persona usuària que requereixi l'accés a alguna pàgina amb accés restringit haurà de sol·licitar-ho a la Comissió de Seguretat.

3. En el cas que es detectin indicis fonamentats d'un ús inadequat de l'accés a internet, l'Ajuntament podrà dur a terme un seguiment de l'adequada utilització d'aquests recursos per part de les persones usuàries.

4.12 INSTAL·LACIÓ I CONFIGURACIÓ DELS EQUIPAMENTS INFORMÀTICS

1. La instal·lació i/o configuració de maquinari i programari corporatiu és competència del personal d'Informàtica.

2. Les persones usuàries no poden modificar la configuració dels equips assignats, llevat d'aquells aspectes de personalització que no afectin a la configuració dels equips. Qualsevol modificació en la configuració dels accessos o programari haurà de ser realitzada pel personal de sistemes designat per l'Ajuntament.

3. Per a la configuració dels accessos a la xarxa o el correu electrònic de l'Ajuntament mitjançant dispositius que siguin propietat de la persona usuària caldrà comptar amb autorització de la Comissió de Seguretat.

4.13 PROPIETAT INTEL·LECTUAL I INDUSTRIAL

Està estrictament prohibit fer ús de programes informàtics sense la corresponent llicència, així com l'ús, la reproducció, la cessió, la transformació o la comunicació pública de qualsevol tipus d'obra o invenció protegida per la propietat intel·lectual o industrial.

4.14 INCIDENTS DE SEGURETAT

1. S'entén per incidència 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 cintes de suport, avaries als aparells i a les connexions de xarxa, etc.

2. És obligació de tota persona usuària comunicar qualsevol incidència que es detecti durant el tractament de dades personals a les quals tinguin accés. Les incidències seran comunicades mitjançant l'adreça de correu electrònic. 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).

3. La comunicació d'incidències de seguretat de dades haurà de ser comunicada en un termini de temps no superior a una hora (1), des del moment en què es conegui la incidència.

4.15 PROTECCIÓ DE DADES

Per a crear nous tractaments de dades personals caldrà posar-ho en coneixement del Delegat de Protecció de Dades mitjançant l'adreça de correu electrònic, per tal que en aquest àmbit es valori la sol·licitud i es doni la autorització si correspon.

4.16 TRACTAMENTS TEMPORALS

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

2. Els tractaments temporals hauran de mantenir les normes de seguretat de la mateixa manera que es mantenen per als tractaments originals.

3. Un tractament temporal mantindrà la mateixa finalitat amb la qual va ser definit el tractament original.

4. Un cop finalitzada la vida útil del tractament temporal haurà de ser eliminat.

4.17 TRACTAMENTS EN SUPORTS NO AUTOMATITZATS (DOCUMENTACIÓ PAPER)

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

2. Només es podrà accedir a la documentació del propi àmbit en el que es desenvolupi l'activitat.

3. La documentació serà tractada amb els criteris d'arxiu, emmagatzematge i destrucció que determinin els criteris arxivístics establerts per l'Ajuntament.

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

5. És d'obligat compliment cuidar que els documents tractats no es destrueixin o es deteriorin.

6. Queda expressament prohibit la divulgació dels documents sense l'autorització de la Comissió de Seguretat.

4.18 DESTRUCCIÓ DE SUPORTS

1. Un cop acabada la vigència legal i les necessitats de tractament de l'entitat, els suports que continguin dades de caràcter personal hauran de ser destruïts de forma controlada.

2. Quan els tractaments siguin automatitzats es comunicarà a la Comissió de Seguretat la seva obsolescència, i serà aquest òrgan qui aplicarà les mesures necessàries per tal de destruir-lo.

3. En el cas de tractaments no automatitzats serà responsabilitat de cada persona usuària la correcta aplicació de les mesures per tal que la informació no sigui recuperable, segons les indicacions del responsable d'àmbit i d'acord els criteris determinats per la Comissió de Seguretat.

4.19 UTILITZACIÓ DELS DISPOSITIUS PORTÀTILS CORPORATIUS (TELÈFONS MÒBILS, TAULETES)

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

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

3. La utilització d'aquests dispositius que permetin la connectivitat per a trucades i consum de dades mòbils es limitarà a allò que tingui relació amb les funcions desenvolupades amb el lloc de treball de la persona usuària, i pel sistema de presència/fitxatge, reservant-se l'Ajuntament el dret a portar a terme aquelles accions de control que siguin necessàries per a garantir-ne un bon ús.

5 COMUNICACIÓ

1. Les persones que entrin a prestar servei a l'Ajuntament, amb caràcter temporal o indefinit, procediran a rebre, formalment i de forma individualitzada, aquest document de prestar serveis l'Ajuntament.

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

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

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

• 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.).

4.En aquestes accions, participen tots els 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 Responsables de les àrees.

6 RESPONSABILITAT

1. L'incompliment per part del personal de les obligacions al servei de l'Ajuntament, serà sancionat disciplinàriament, d'acord amb la gravetat de l'incompliment i d'acord amb el que disposa el Reial Decret Legislatiu 5/2015, 30 d'octubre, pel qual s'aprova el text refós de la Llei de l'Estatut Bàsic de l'Empleat Públic i la normativa que derivi del mateix.

2. La responsabilitat penal derivada del delicte en què hagi incorregut el personal al servei de l'Ajuntament, s'exigirà de conformitat amb la legislació corresponent.