

**PROCEDURA DIPARTIMENTO ICT**  
**ATS SARDEGNA**

**SICUREZZA INFORMATICA DEI**  
**SISTEMI E DELL'INFRASTRUTTURA**  
**DI RETE**

Data:	<b>10-12-2018</b>
Autore:	Marco Galisai
Versione-Variante	003-A
Rivisto:	Marco Galisai
Approvato:	Marco Galisai Mauro Gaviano Marco Fenudi Maurizio Medda
Distribuito:	Personale Dipartimento ICT – ATS Sardegna

## ELEMENTI DI CONTROLLO DEL DOCUMENTO

**Sintesi:** Descrive la procedura di conduzione, gestione delle attività e misure di sicurezza fisica e logica per i Sistemi Informativi della ATS Sardegna.

<b>Codice</b>	DDICT-PD-SI-003.A
<b>Tipo</b>	Procedura Dipartimentale
<b>Data</b>	10-12-2018
<b>Versione</b>	003
<b>Variante</b>	A
<b>Stato</b>	<i>Definitivo</i>
<b>Pagine</b>	75
<b>Altri documenti correlati</b>	<ul style="list-style-type: none"><li>- Deliberazione del Direttore Generale n. 373 del 09/03/2018 avente per oggetto "Attivazione, in via provvisoria e temporanea, del Dipartimento ICT"</li><li>- Ordine di Servizio del Dipartimento ICT (rif. NP/2018/23124 del 26/03/2018) avente per oggetto "DIPARTIMENTO ICT - Ordine di Servizio N. 1 – Allocazione iniziale del personale alle Strutture Complesse del Dipartimento ICT e prime indicazioni operative"</li><li>- Deliberazione del Direttore Generale n. 183 del 06/02/2018 avente per oggetto: "Adozione del Piano Triennale 2018 – 2020 di Sviluppo del Sistema Informativo dell'Azienda di Tutela della Salute della Sardegna"</li><li>- Regolamento UE n. 679/2016 sulla Protezione dei Dati Personali – GDPR</li><li>- Decreto Legislativo n. 196 del 2003 "Codice in materia di protezione dei dati personali"</li><li>- AgID - CIRCOLARE 18 aprile 2017, n. 2/2017</li><li>- AgID - Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017 – 2019</li><li>- Regolamento per la protezione dei dati personali dell'Azienda per la tutela della Salute – ATS Sardegna</li><li>- ISO/IEC 27002:2013 – Second Edition – <i>Information Technology, Security Techniques, Code of Practice for Information Security Controls</i></li><li>- 2014 Italian Cyber Security Report – <i>Consapevolezza della minaccia e capacità difensiva della pubblica amministrazione italiana</i> – Research Center of Cyber Intelligence and Information Security "Sapienza" Università di Roma</li><li>- Standard documentazione Dipartimento ICT - <i>DDICT-LG-DD-001.C</i> del 13/06/2018</li></ul>

<b>Moduli</b>	Non applicabile
<b>Parole Chiave</b>	<ul style="list-style-type: none"><li>▪ Catalogo dei Documenti</li><li>▪ Sicurezza Fisica</li><li>▪ Sicurezza Logica</li><li>▪ GDPR</li><li>▪ Registro dei Trattamenti</li><li>▪ Misure Minime di Sicurezza</li></ul>
<b>File Name</b>	Procedura_Sicurezza_Informatica_Sistemi_E_Infrastruttura_Di_Rete.docx

**Evoluzione modifiche apportate:**

<b>Data</b>	<b>Versione/Variante</b>	<b>Descrizione</b>
31-07-2018	A	Versione iniziale
04-09-2018	B	<ul style="list-style-type: none"><li>▪ Revisione _____</li><li>▪ Revisione _____</li><li>▪ Revisione _____</li></ul>
10/12/2018	C	Approvazione del documento

## INDICE

<b>1.</b>	<b>INTRODUZIONE.....</b>	<b>7</b>
1.1.	PREMESSA.....	7
1.2.	OGGETTO.....	10
1.3.	AREA DI APPLICAZIONE.....	12
1.3.1.	<i>Integrazione Infrastruttura di Rete - ATS Sardegna.....</i>	<i>13</i>
1.3.2.	<i>Infrastruttura Telefonica.....</i>	<i>14</i>
1.3.3.	<i>Sistemi e Dotazioni .....</i>	<i>15</i>
1.3.4.	<i>Mappa Infrastruttura Tecnologica ATS Sardegna .....</i>	<i>15</i>
1.3.5.	<i>Sintesi degli Aspetti Applicativi ATS Sardegna.....</i>	<i>17</i>
1.4.	ABBREVIAZIONI E ACRONIMI.....	19
<b>2.</b>	<b>AMBITO DI SICUREZZA E PRIVACY.....</b>	<b>20</b>
2.1.	INSIEME DELLE MISURE DI SICUREZZA .....	20
2.2.	POLITICHE DI ATTUAZIONE DELLA SICUREZZA – ATS SARDEGNA .....	21
2.3.	STRATEGIE E MISURE DI SICUREZZA.....	22
2.4.	DELEGATI AL TRATTAMENTO DATI E FIGURE DI RIFERIMENTO .....	23
2.5.	ASPETTI GENERALI DEL TRATTAMENTO DATI – DIRETTIVE ED ISTRUZIONI.....	24
2.5.1.	<i>Modalità di Trattamento e Raccolta dei Dati Personali .....</i>	<i>24</i>
2.5.2.	<i>Cautele per i Dati “sensibili”, giudiziari, etc.....</i>	<i>25</i>
2.5.3.	<i>Affidamento dei Dati Personali all’Esterno.....</i>	<i>26</i>
2.6.	REGISTRO DEI TRATTAMENTI – ART. 30 REGOLAMENTO UE 679/2016 - GDPR.....	28
2.6.1.	<i>Riferimento Normativo.....</i>	<i>28</i>
2.6.2.	<i>Contenuti del Registro .....</i>	<i>29</i>
2.7.	DEFINIZIONI.....	31
<b>3.</b>	<b>LA GESTIONE DELLA SICUREZZA .....</b>	<b>34</b>
3.1.	AGID – MISURE MINIME DI SICUREZZA .....	34
3.1.1.	<i>Classi delle Misure Minime – Esempio.....</i>	<i>36</i>
3.1.2.	<i>Attuazione Misure Minime – ATS Sardegna .....</i>	<i>37</i>
3.1.3.	<i>Criticità e Aspetti di Controllo sulle Misure Minime di Sicurezza – ATS Sardegna .....</i>	<i>37</i>
3.2.	ASPETTI RELATIVI ALLA SICUREZZA FISICA.....	39
3.2.1.	<i>Protezione delle Aree e dei Locali .....</i>	<i>40</i>
3.2.2.	<i>Ubicazione di Sistemi e Apparati della Piattaforma Tecnologica .....</i>	<i>41</i>
3.2.3.	<i>Collocazione delle Stazioni di Lavoro .....</i>	<i>42</i>
3.2.4.	<i>Salvataggio dei Dati.....</i>	<i>42</i>
3.3.	CUSTODIA E ARCHIVIAZIONE DI ATTI, DOCUMENTI E SUPPORTI .....	43
3.4.	MISURE LOGICHE DI SICUREZZA.....	44
3.4.1.	<i>Credenziali Utente – Autenticazione e Profilazione .....</i>	<i>45</i>
3.4.1.1.	<i>La disattivazione delle credenziali di autenticazione .....</i>	<i>46</i>
3.4.1.2.	<i>Le Istruzioni agli Utenti .....</i>	<i>46</i>
3.4.1.3.	<i>La gestione password in deroga.....</i>	<i>46</i>
3.4.1.4.	<i>I profili di autorizzazione.....</i>	<i>47</i>
3.4.1.5.	<i>La verifica periodica di sussistenza .....</i>	<i>47</i>
3.4.2.	<i>Protezione anti-intrusione e anti-malware .....</i>	<i>47</i>
3.4.3.	<i>Gestione dei Supporti Fisici Rimovibili .....</i>	<i>48</i>
3.5.	UTILIZZO DELLE RISORSE INFORMATICHE AZIENDALI.....	48
3.5.1.	<i>Accesso alle Risorse ICT .....</i>	<i>49</i>
3.5.2.	<i>Utilizzo delle Credenziali di Autenticazione .....</i>	<i>49</i>

3.5.2.1.	Regole definizione e gestione della password: .....	50
3.5.3.	<i>Utilizzo delle Postazioni di Lavoro</i> .....	51
3.6.	UTILIZZO DEI SERVIZI ICT AZIENDALI.....	52
3.6.1.	<i>Servizi della Rete Internet</i> .....	52
3.6.1.1.	Autorizzazione all'uso della rete Internet .....	52
3.6.1.2.	Uso della rete Internet.....	52
3.6.1.3.	Comportamento durante l'accesso ad Internet.....	52
3.6.1.4.	Trasferimento di dati e/o programmi da Internet .....	53
3.6.1.5.	Collegamento ad Internet.....	53
3.6.1.6.	Monitoraggio automatico .....	53
3.6.1.7.	Filtri di navigazione .....	53
3.6.1.8.	Modalità di controllo .....	54
3.6.2.	<i>Servizi di Posta elettronica</i> .....	54
3.6.2.1.	Titolarità della posta elettronica.....	54
3.6.2.2.	Principi generali .....	54
3.6.2.3.	Uso della posta elettronica Aziendale.....	55
3.6.2.4.	Uso non adeguato della posta elettronica .....	56
-3.6.2.5.	Responsabilità dell'utente .....	56
3.6.2.6.	Raccomandazione sull'invio di dati sensibili o giudiziari .....	56
3.6.2.7.	Disclaimer .....	56
3.6.2.8.	Segretezza e riservatezza .....	57
3.6.2.9.	Responsabilità dell'utente per dati trasmessi via posta elettronica .....	57
3.6.2.10.	False Dichiarazioni e utilizzo profili impropri .....	57
3.6.2.11.	Conservazione e cancellazione della posta elettronica.....	57
3.6.2.12.	Interruzione della consegna di posta elettronica.....	57
3.6.2.13.	Modalità di controllo.....	57
3.6.2.14.	Caratteristiche della casella di posta.....	58
3.6.2.15.	Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica .....	59
3.6.2.16.	Segnalazione incidenti / intrusioni .....	59
3.6.3.	<i>Servizi Mobile e postazioni personali</i> .....	59
<b>4.</b>	<b>INFRASTRUTTURA RETE TELEMATICA ATS</b> .....	<b>61</b>
4.1.	INFRASTRUTTURA RETE DATI E TELEFONICA ATS .....	61
4.2.	SICUREZZA FISICA E LOGICA.....	63
4.3.	INTERCONNESSIONE DELLE RETI DATI DELLE SINGOLE ASSL .....	64
4.4.	STRUMENTI – APPARATI DI RETE .....	65
4.5.	SICUREZZA PERIMETRALE E GESTIONE DELLE VULNERABILITÀ .....	66
4.6.	ORGANIZZAZIONE E MODALITÀ DI GESTIONE DELL'INFRASTRUTTURA DI NETWORKING .....	66
<b>5.</b>	<b>REGOLE PER L'UTILIZZO DELLA RETE TELEMATICA AZIENDALE</b> .....	<b>68</b>
5.1.	REGOLE PER L'UTILIZZO CORRETTO DELLA CONNESSIONE ALLA RETE AZIENDALE .....	68
5.2.	REGOLE COMPORTAMENTALI PER L'USO DELL'ACCESSO DA REMOTO ALLA RETE AZIENDALE (VPN) .....	71
5.3.	REGOLE COMPORTAMENTALI PER L'UTILIZZO DI DISPOSITIVI PORTATILI E PERSONALI AUTORIZZATI COLLEGATI ALLA RETE AZIENDALE .....	72
5.4.	REGOLE COMPORTAMENTALI PER LA CONNESSIONE ALLA RETE AZIENDALE DI APPARECCHIATURE ELETTRONICHE FORNITE DA DITTE ESTERNE .....	74
<b>6.</b>	<b>RUOLI E RESPONSABILITÀ</b> .....	<b>75</b>
6.1.	IL MONITORAGGIO E CONTROLLO SULLO STATO DELLA SICUREZZA.....	76
<b>7.</b>	<b>REQUISITI E VINCOLI</b> .....	<b>78</b>
<b>8.</b>	<b>NORME E STANDARD</b> .....	<b>79</b>
<b>9.</b>	<b>STRUTTURA DI RIFERIMENTO</b> .....	<b>80</b>

**10. TECNICHE E STRUMENTI.....82**

## INDICE delle Tabelle

TABELLA 1 – SISTEMI E DOTAZIONI	15
TABELLA 2 – MAPPA INFRASTRUTTURE TECNOLOGICHE	17
TABELLA 3 – ABBREVIAZIONI E ACRONIMI	19
TABELLA 4 – DEFINIZIONI GDPR	32
TABELLA 5 – AGID – MISURE MINIME DI SICUREZZA	34
TABELLA 6 – CLASSI MISURE DI SICUREZZA	35
TABELLA 7 – ASPETTI DI CONTROLLO E CRITICITÀ - MISURE DI SICUREZZA	39
TABELLA 8 – ISO/IEC 27002:2013 - <i>SECURITY POLICIES AND CONTROLS</i>	41
TABELLA 9 – CREDENZIALI: ISTRUZIONI PER GLI UTENTI	46
TABELLA 10 – VINCOLI E REQUISITI	78
TABELLA 11 – SERVIZI DI SICUREZZA – STRUMENTI E METODI	89

## INDICE delle Figure

FIGURA 1 - MODELLO STRATEGICO DI EVOLUZIONE DEL SISTEMA INFORMATIVO DELLA PA – AGID	8
FIGURA 2 – ANALISI DATI PA ITALIANA - RISULTATI PER CATEGORIA	9
FIGURA 3 – NUMERO TENTATIVI DI ATTACCO NEL 2013	9
FIGURA 4 - ARCHITETTURA DI RETE – ATS SARDEGNA	13
FIGURA 5 – SCHEMA ARCHITETTURA RETE TELEFONICA – ESEMPLIFICATIVO – ATS SARDEGNA	14
FIGURA 6 - ARCHITETTURA APPLICATIVA DEL SISTEMA SANITARIO REGIONALE	18
FIGURA 7 - INFRASTRUTTURE APPLICATIVE (EX-ASL-AO)	18
FIGURA 8 – CLASSE MISURE MINIME – CIRCOLARE AGID - ALLEGATO 1 - ABSC1	36
FIGURA 9 – ARCHITETTURA LOGICA COMUNE DEI SERVIZI DI PROTEZIONE	84
FIGURA 10 – ARCHITETTURA SERVIZI DATA LOSS/LEAK PREVENTION	85
FIGURA 11 – ARCHITETTURA SERVIZI DATABASE SECURITY	86
FIGURA 12 – ARCHITETTURA SERVIZIO WEB APPLICATION FIREWALL	87
FIGURA 13 – ARCHITETTURA SERVIZIO SECURE WEB GATEWAY	88

### **3.6.2.15. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica**

L'accesso alla rete internet dal computer aziendale espone l'ente a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'organizzazione stessa.

Una gestione dei dati difforme dalle regole contenute nel presente disciplinare potrebbe esporre l'organizzazione ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.

L'ente impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno settimanale.

L'utente, da parte sua, deve impegnarsi a controllare il corretto funzionamento del proprio computer, e, in particolare, deve rispettare le regole seguenti:

- Comunicare al dipartimento ICT ogni anomalia o malfunzionamento del sistema antivirus;
- Comunicare al dipartimento ICT eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all'incaricato:

- È vietato ostacolare l'azione dell'antivirus aziendale;
- È vietato disattivare l'antivirus senza l'autorizzazione espressa dal dipartimento ICT anche e soprattutto, nel caso sia richiesto per l'installazione di software sul computer;

Contattare il dipartimento ICT prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

### **3.6.2.16. Segnalazione incidenti / intrusioni**

Ogni incidente deve essere segnalato dall'utente in modo tempestivo al dipartimento ICT, che raccoglierà le segnalazioni e avvierà il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative.

Nel caso l'incidente sia di una certa gravità e riguardi il patrimonio informativo e di conoscenza detenuto dall'Azienda, oppure le applicazioni informatiche, l'utente dovrà avvisare anche il Responsabile del dipartimento ICT di riferimento/appartenenza.

Per gli incidenti che possono determinare una violazione dei dati personali, cioè la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, l'utente avvisa senza indugio il Responsabile del Dipartimento ICT, segnala anche le violazioni o gli incidenti informatici che ha rilevato e che possono avere un impatto significativo sui dati personali.

### **3.6.3. Servizi Mobile e postazioni personali**

Per gli utenti che utilizzano postazioni mobili (tablet, smart-fone, laptop, ecc..) o postazioni personali private per accedere alla casella mail aziendale si raccomanda quanto segue:

- Non memorizzare le password nella postazione di lavoro;
- Non condividere la postazione di lavoro con familiari e/o amici;
- Tenere sempre aggiornato un sistema di protezione antivirus e contro i malware;
- Non utilizzare la medesima password di accesso alla casella mail aziendale per accedere a sistemi di web social network.