PROCEDURA DIPARTIMENTO ICT

ATS SARDEGNA

SICUREZZA INFORMATICA DEI SISTEMI E DELL'INFRASTRUTTURA DI RETE

Data:	**10-12-2018**
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.

Codice	DDICT-PD-SI-003.A
Tipo	Procedura Dipartimentale
Data	10-12-2018
Versione	003
Variante	A
Stato	*Definitivo*
Pagine	75
Altri documenti correlati	– Deliberazione del Direttore Generale n. 373 del 09/03/2018 avente per oggetto "*Attivazione, in via provvisoria e temporanea, del Dipartimento ICT*" – 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*" – 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*" – Regolamento UE n. 679/2016 sulla Protezione dei Dati Personali – GDPR – Decreto Legislativo n. 196 del 2003 "Codice in materia di protezione dei dati personali" – AgID - CIRCOLARE 18 aprile 2017, n. 2/2017 – AgID - Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017 – 2019 – Regolamento per la protezione dei dati personali dell'Azienda per la tutela della Salute – ATS Sardegna – ISO/IEC 27002:2013 – Second Edition – *Information Technology, Security Tecniques, Code of Practice for Information Security Controls* – 2014 Italian Cyber Security Report – *Consapevolezza della minaccia e capacità difensiva ella pubblica amministrazione italiana* – Research Center of Cyber Intelligence and Information Security "Sapienza" Università di Roma – Standard documentazione Dipartimento ICT - *DDICT-LG-DD-001.C* del 13/06/2018

Moduli	Non applicabile
Parole Chiave	▪ Catalogo dei Documenti ▪ Sicurezza Fisica ▪ Sicurezza Logica ▪ GDPR ▪ Registro dei Trattamenti ▪ Misure Minime di Sicurezza
File Name	Procedura_Sicurezza_Informatica_Sistemi_E_Infrastruttura_Di_Rete.docx

Evoluzione modifiche apportate:

Data	Versione/Variante	Descrizione
31-07-2018	A	Versione iniziale
04-09-2018	B	▪ Revisione _____ ▪ Revisione _____ ▪ Revisione _____
10/12/2018	C	Approvazione del documento

INDICE

INDICE delle Tabelle

INDICE delle Figure

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.