SOMMARIO

REVISIONI		
ED. REV.	DATA APPROV.	DESCRIZIONE
		1° Emissione

Emissione	Approvazione
RSGDP	**DIR / DPO**

1.Scopo

La presente procedura ha lo scopo di definire specifiche riportate per le politiche di sicurezza adottate dal sistema .

2.Applicabilità

La presente procedura si applica a tutte le attività interessate al SGDP

3.Riferimenti

Sistema SGDP

4.Responsabilità ed aggiornamento

La responsabilità dell'applicazione della presente procedura è del RSGDP.

5.Modalità operative

5.1.1 Politica di gestione della sicurezza del SGDP

La gestione in sicurezza delle infrastrutture informatiche ha l'obiettivo di garantire che i sistemi, le postazioni di lavoro, le applicazioni, i servizi di rete, i servizi elaborativi forniscano le prestazioni elaborative ai livelli e con i requisiti di sicurezza definiti.
Vengono inoltre di seguito sintetizzati i principi generali in base ai quali porre in essere la gestione sicura dei sistemi:

- Viene gestito ed aggiornato un inventario degli asset hardware e software;
- Vengono applicate regole standard per la installazione e la configurazione dei sistemi;
- le configurazioni dei sistemi sono disegnate tenendo in considerazione le esigenze attuali e future delle prestazioni;
- le configurazioni dei sistemi sono indirizzare nel modo più compiuto possibile la sicurezza built- in e facilitano l'installazione di ulteriori misure di sicurezza;
- sono adottate procedure standard di configurazione dei sistemi che indirizzino:
    - disabilitazione o restrizione nell'utilizzo di alcuni particolari servizi;
    - restrizioni nell'accesso ad utilities di sistema particolarmente critiche ed a funzioni di setting di sistema;
    - utilizzo di funzioni di time-out;

- le principali esigenze di aggiornamenti in termini di patch e di fix di sicurezza;

- le configurazioni dei sistemi sono archiviate ed aggiornate all'interno di un fascicolo governato centralmente;
- sono condotte regolarmente attività di monitoraggio sulle prestazioni dei sistemi al fine di gestire adeguatamente eventi, problemi e incidenti.

E' predisposta un'adeguata politica di backup, eventualmente anche remoto, che naturalmente sia in accordo e coerenza con quanto previsto dal manuale della conservazione.

Politica di sicurezza dei Fornitori.

Per quanto riguarda la definizione di standard di sicurezza da sottoporre ai fornitori di servizi che possano avere un ruolo determinante nell'ambito del SGDP, sono previste per ciascuno apposite lettere di incarico con le specifiche da attuare nell'ambito della tipologia dei dati da trattare per conto dell'Organizzazione. Tale trattamento deve essere garantito con adeguate misure di sicurezza da adottare da parte degli stessi fornitori.

5.1.2 Politica per il controllo degli accessi fisici

Sono presenti adeguate modalità di controllo degli accessi fisici, che prevedano, le seguenti classi di accesso:

- personale dell'organizzazione;
- personale di fornitori esterni;
- personale della/delle amministrazione/amministrazioni servite dal sistema;
- personale delegato dall'organizzazione (a esempio personale che esegue manutenzione/riparazione, ecc.).

5.1.3 Politica per l'inserimento dell'utenza e per il controllo degli accessi logici

Le modalità di inserimento dell'utenza sul sistema informativo dell'Organizzazione, viene attribuito all'Amministratore di sistema (o nel caso non sia previsto dal

responsabile del SGDP), compresa l'attribuzione delle autorizzazioni per gli accessi a sistemi, applicazioni e applicativi dell'organizzazione;
L'Amministratore provvede anche a definire le modalità di cancellazione o di cambio di autorizzazione, con specifico riferimento al sistema di conservazione documentale.

5.1.4 Politica di gestione delle postazioni di lavoro

Gli elementi essenziali di questa politica sono:

- elementi minimi previsti per definizione delle "postazioni di lavoro";
- regole per l'installazione del software sulle postazioni di lavoro;
- regole per gli aggiornamenti;
- regole per la limitazione della connettività a supporti esterni (CD/DVD, Pen Drive, ecc.);
- regole per la modifica delle impostazioni.

Tale attività vengono definite ed attuate dall'Amministratore di sistema (o nel caso non sia previsto dal responsabile del SGDP).

5.1.5 Politica di gestione dei contenuti applicativi

Le attività riguardo la manutenzione dei sistemi, il controllo sul contenuto software dei client al fine di verificare l'assenza di codice malevolo e la conformità a quanto autorizzato e previsto dalle licenze d'uso, viene svolto da parte dell'Amministratore di sistema (o nel caso non sia previsto dal Resp Manutenzione Strumenti Elettronici - RMSE).

5.1.6 Politica di gestione, dismissione e smaltimento degli apparati mobili e dei supporti

Particolare attenzione viene posta alla gestione degli apparati mobili (portatili, tablet, smartphone, cellulari, ecc.) e dei supporti esterni ai server e alle postazioni di lavoro quali, a esempio: HD esterni/CD/DVD/Pen Drive/DAT/LTO, ecc., ma anche carta stampata, che siano utilizzati e/o prodotti nell'ambito delle attività di conservazione documentale.

L'Amministratore di sistema (o nel caso non sia previsto dal Resp Manutenzione Strumenti Elettronici - RMSE) definisce le regole, oltre che le modalità di utilizzo e conservazione dei dispositivi, anche quelle per la dismissione/distruzione degli apparati e dei supporti.

5.1.7 Politica di gestione dei canali di comunicazione

I canali di comunicazione, quali e-mail, sistemi di instant messaging, VoIP, internet, accessi wireless, fax, scanner, fotocopiatrici sono controllati al fine di preservare la confidenzialità, e l'integrità delle informazioni in transito, ed allo stesso tempo ad impedire l'abuso che si potrebbe fare di tali strumenti di comunicazione.
Di conseguenza la tipologia di controlli copre le problematiche di utilizzo appropriato dello strumento, le problematiche di comportamento dell'utilizzatore dello strumento e le tecnologie coinvolte.

5.1.8 Manutenzione delle politiche di sicurezza

Viene previsto il perfezionamento, la divulgazione e il riesame delle politiche di sicurezza al verificarsi dei seguenti casi:

- incidenti di sicurezza;
- variazioni tecnologiche significative;
- modifiche all'architettura informatica;
- aggiornamenti delle prescrizioni normative;
- risultati delle eventuali attività di audit interni.

A tal proposito si prevede adeguata formazione a tutto il personale dell'Organizzazione periodicamente.