- POLITICA SULLA SICUREZZA DELLE INFORMAZIONI DEL SERVIZIO DI CONSERVAZIONE DIGITALE -

	Data	*Nominativo*	*Funzione*
Redazione	09/11/2020	HSPI	Consulenti esterni
Verifica	30/11/2020	Armando Tomasi Luca Surace Luca Lanaro	Comitato della Sicurezza delle Informazioni
Approvazione	30/11/2020	Armando Tomasi	Direzione

SOMMARIO

Elenco delle modifiche

Storia delle modifiche apportate al documento		
Versione	Variazioni	Data
1.0	Prima emissione	30/11/2020

Livello di riservatezza del documento

Pubblico

1 INTRODUZIONE

Questo documento costituisce il quadro generale di riferimento della Provincia Autonoma di Trento (PAT) rispetto alle politiche di sicurezza delle informazioni implementate da PAT **per assicurare una corretta gestione della sicurezza del Servizio di Conservazione dei documenti digitali**.

2 STANDARD E DOCUMENTI DI RIFERIMENTO

L'elenco aggiornato degli standard e dei documenti di riferimento è contenuto nel documento *Normativa applicabile*.

3 PROFILO DI MINACCIA

Un aspetto particolarmente critico del servizio, data la sua natura, è la **sicurezza dei documenti**. Infatti, il Servizio di Conservazione comporta l'archiviazione di informazioni di varia natura e importanza, alcune di particolare criticità per il carattere di riservatezza o unicità che le caratterizza (ad esempio documenti contenenti dati particolari).

In generale, le minacce a cui deve far fronte PAT, sono riassumibili nelle seguenti (*elenco non esaustivo*):

- accesso e/o diffusione non autorizzata di documenti, anche contenenti informazioni personali/particolari (requisito minacciato: riservatezza);
- archiviazione di un dato/documento non corretto (requisito minacciato: integrità);
- perdita di documenti (requisito minacciato: integrità);
- alterazione delle informazioni contenute nei documenti (requisito minacciato: autenticità);
- indisponibilità del servizio di conservazione dei documenti (requisito minacciato: disponibilità).

4 POLITICHE

Le politiche per la sicurezza delle informazioni si applicano a **tutto il ciclo di vita del Servizio di Conservazione** dalla fase di attivazione, attraverso la fase di esercizio (immissione, gestione e messa a disposizione dei documenti), fino all'eventuale fase di cessazione del servizio, nonché alle connesse attività di natura tecnologica gestite dal Polo archivistico regionale (ParER), di seguito definito come Gestore dell'Infrastruttura.

Esse **interessano**, in generale, il **personale PAT addetto alle funzioni di conservazione**, con l'intento di assicurare la protezione delle informazioni in ogni passaggio dei trattamenti operati e per l'intero ciclo di vita delle informazioni stesse.

4.1 USO ACCETTABILE DEGLI ASSET

4.1.1 Obiettivo

L'obiettivo della seguente politica è indirizzare i **comportamenti degli utenti** relativamente agli asset utilizzati, allo scopo di prevenire l'accesso non autorizzato ai documenti.

4.1.2 Riferimenti esterni:

PAT fa riferimento:

- alla propria Delibera n. 54 del 25 gennaio 2019 – con allegato dal titolo "Privacy & Digital Policy Della Provincia Autonoma di Trento" - in materia di sicurezza e privacy, pubblicata sul sito web istituzionale; in particolare si considerano i Capitoli:
  - 3.2 Prescrizioni operative finalizzate alla riduzione dei rischi (Misure di sicurezza organizzative);
  - 8. Misure di sicurezza relative alle risorse di rete e dei PC;
  - 9. Misure di sicurezza relative alle postazioni di lavoro;
  - 11. Misure di sicurezza relative ad internet.
- al Disciplinare per l'utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche.

4.1.3 Regole/requisiti:

Tutto il personale deve:

- essere a conoscenza del proprio ruolo e delle responsabilità nel contribuire ad un corretto e sicuro utilizzo delle risorse informative. In particolare, ognuno è responsabile della protezione e della conservazione dei beni della Provincia, materiali e immateriali, avuti in affidamento per l'espletamento dei propri compiti, nonché del loro utilizzo in modo proprio e conforme ai fini della Provincia;
- proteggere i computer e le altre strumentazioni informatiche, in caso di assenza, anche temporanea, dalla postazione di lavoro, tramite la sospensione o il blocco della sessione di lavoro;
- utilizzare sulle postazioni di lavoro esclusivamente il software autorizzato e fornito dalla Provincia;
- segnalare sempre, in ogni caso e preventivamente al proprio referente informatico, la necessità di installare eventuale software aggiuntivo rispetto all'installazione standard, anche se gratuito e necessario per lo svolgimento dell'attività lavorativa;
- utilizzare stampanti in cui è attiva la funzionalità di stampa riservata e il rilascio della stampa è subordinata alla presenza dell'utente presso la stampante; ciò allo scopo di mantenere la riservatezza dei documenti stampati;
- evitare di archiviare nel proprio computer i documenti informatici conservati nel Sistema di Conservazione, se non per il tempo strettamente necessario per svolgere l'attività di esibizione;
- evitare di lasciare informazioni ritenute strategiche e/o sensibili (su supporto cartaceo e/o elettronico) dove possono essere lette, copiate e sottratte da personale non autorizzato e procedere allo smaltimento sicuro (es. distruzione) dei supporti cartacei contenenti tali informazioni quando essi non siano più necessari;
- è vietato l'utilizzo di dispositivi mobili e supporti rimovibili (CD, hard disk, ecc.) relativamente alle attività di versamento, gestione e distribuzione di documenti in conservazione;
- impegnarsi ad adottare tutte le misure di sicurezza definite nella presente politica nella gestione dei dispositivi portatili con particolare riferimento alle trasferte lavorative o alle attività di fuori del luogo di lavoro.

4.2 RISORSE UMANE

4.2.1 Obiettivo

L'obiettivo della seguente politica è garantire che il personale di PAT addetto alle funzioni di conservazione (dipendenti e collaboratori) abbia **piena consapevolezza delle problematiche relative alla sicurezza delle informazioni**. Perciò PAT applica nei confronti di tutte le persone coinvolte nel processo di conservazione (personale interno coinvolto, fornitori e altre terze parti) gli indirizzi generali sulla sicurezza, affinché:

- comprendano l'importanza degli indirizzi generali, delle politiche e delle procedure adottate da PAT per assicurare la sicurezza delle informazioni;
- comprendano il loro ruolo all'interno del sistema di conservazione, con particolare riferimento alle problematiche della sicurezza;
- siano informati sui comportamenti da tenere per assicurare gli opportuni livelli di sicurezza.

4.2.2 Riferimenti esterni:

PAT fa riferimento alla Legge Provinciale Numero 7 del 1997 che disciplina il sistema organizzativo provinciale e il rapporto di lavoro del personale della Provincia e degli enti funzionali dalla stessa dipendenti.

4.2.3 Regole/requisiti:

Nella fase di selezione e per tutta la durata del rapporto di lavoro:

- devono essere valutati i livelli di affidabilità, competenza e conoscenza degli obiettivi e delle problematiche di sicurezza dell'organizzazione in funzione delle attività che dovranno essere svolte;
- devono essere chiaramente comunicati (e sottoscritti dal soggetto) gli eventuali obblighi di riservatezza per i quali viene richiesto l'impegno; va altresì specificato se tali obblighi permangono anche a valle della cessazione del rapporto di lavoro;
- il personale deve ricevere un'adeguata e continuativa formazione inerente le tematiche di sicurezza e privacy dei dati, con particolare riferimento a:
  - politiche e procedure in materia di sicurezza delle informazioni;
  - principali rischi che insistono su dati e informazioni;
  - misure disponibili per prevenire eventi dannosi;
  - obblighi legislativi, regolamentari e contrattuali in materia di informazione e trattamento e protezione dei dati (con particolare riferimento ai dati degli enti convenzionati);
- le modalità di chiusura del rapporto di lavoro con PAT devono assicurare la corretta rimozione dei diritti di accesso alle risorse informative nonché la restituzione di tutti i beni forniti in uso al personale.

4.3 GESTIONE TERZE PARTI

4.3.1 Obiettivo

L'obiettivo della presente politica è **assicurare la conformità ai requisiti legali e ai principi legati alla sicurezza delle informazioni nei contratti con le terze parti, compreso il Gestore dell'Infrastruttura**, in accordo con le caratteristiche specifiche della relazione che PAT deve instaurare con le terze parti stesse.

4.3.2 Riferimenti esterni:

N.A.

4.3.3 Regole/requisiti:

Gli accordi con le terze parti che accedono alle informazioni e/o agli strumenti che le elaborano:

- devono essere basati su contratti formali contenenti opportuni requisiti di sicurezza. I requisiti di sicurezza devono risultare adeguati rispetto ai rischi, accidentali e/o intenzionali, di distruzione, perdita, divulgazione, alterazione e accesso non autorizzato delle risorse informative dell'organizzazione;
- devono garantire il rispetto dei requisiti di legge in materia di protezione dei dati personali e copyright delle risorse informative accedute e utilizzate.
- devono prevedere accordi per garantire la riservatezza e la non-divulgazione delle informazioni critiche dell'organizzazione. Tali accordi devono necessariamente contemplare tutti i requisiti dell'organizzazione definiti per assicurare la protezione delle risorse informative;
- devono includere, ove possibile, la possibilità di effettuare attività di audit di II parte sui fornitori per verificare il rispetto dei requisiti di sicurezza concordati.

4.4 GESTIONE DEGLI ASSET

4.4.1 Obiettivo

L'obiettivo della presente politica è **assicurare che tutti gli asset associati al servizio di conservazione** siano stati opportunamente **identificati e inventariati**, che sia stato **individuato un responsabile** al fine di gestire le minacce associate alla sicurezza delle informazioni e che siano definite le politiche per la **dismissione sicura degli asset**.

4.4.2 Riferimenti esterni:

PAT fa riferimento alla propria Delibera n. 54 del 25 gennaio 2019 – con allegato dal titolo "Privacy & Digital Policy Della Provincia Autonoma di Trento" - in materia di sicurezza e privacy, pubblicata sul sito web istituzionale; in particolare si considera il Capitolo 9.3.2 Dismissione della postazione di lavoro della Delibera n. 54 del 2019.

Per ciò che attiene agli asset relativi al Sistema di conservazione SacER, si rimanda alle policy adottate dal Gestore dell'Infrastruttura e in particolare alla "Politica sulla sicurezza delle informazioni del servizio di conservazione di ParER".

4.4.3 Regole/requisiti:

- ai fini della selezione e attuazione di adeguati meccanismi di controllo, le informazioni gestite devono essere identificate e classificate:
  - in ordine al grado di sensibilità e criticità;
  - al fine di distinguere precisamente le informazioni di proprietà di tutti gli attori coinvolti nel servizio di conservazione, da quelli da essi derivati e/o comunque ricadenti nella sfera di "titolarità" / appartenenza di PAT;
- tutti i componenti tecnologici e organizzativi necessari alla gestione del servizio di conservazione hanno lo stesso grado di classificazione, coerentemente con il fatto che tutte le informazioni sono classificate al medesimo livello;
- ogni qualvolta si dismette un dispositivo elettronico o informatico che contiene dati personali/sensibili, è necessario adottare idonei accorgimenti e misure, anche attraverso soggetti terzi, tecnicamente qualificati, che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle;

In considerazione delle caratteristiche e della missione del servizio, e in relazione al fatto che non è PAT a stabilire la criticità relativa alle informazioni contenute nei documenti conservati (bensì i titolari delle informazioni stesse), si stabilisce che tutte le informazioni contenute nei documenti che saranno affidati a PAT dagli Enti produttori abbiano tutte lo stesso livello di criticità e, pertanto, siano soggette allo stesso grado di protezione.

4.5 Analisi dei Rischi

4.5.1 Obiettivo

L'obiettivo della presente politica è **assicurare che i rischi associati al servizio di conservazione siano identificati, valutati e trattati**.

4.5.2 Riferimenti esterni:

N.A.

4.5.3 Regole/requisiti:

- il sistema di controllo relativo al servizio di conservazione deve essere risk based: l'Analisi dei Rischio è l'elemento principale da cui discendono tutte le attività di controllo, le Politiche in merito alla sicurezza e le procedure operative legate alla sicurezza delle informazioni.
- i necessari controlli per la mitigazione di potenziali rischi devono essere definiti a seguito di un'attività di risk assessment;
- l'attività di risk assessment va ripetuta con cadenza periodica e regolare, a garanzia del permanere dell'efficacia delle misure di mitigazione identificate e attuate.

4.6 Separazione dei ruoli

4.6.1 Obiettivo

L'obiettivo della presente politica è **garantire i necessari livelli di sicurezza nell'esercizio del servizio di conservazione**, attraverso l'attuazione dei principi di separazione dei ruoli.

4.6.2 Riferimenti esterni:

N.A.

4.6.3 Regole/requisiti:

- i principi di separazione dei ruoli e privilegio minimo devono prevedere, almeno, la seguente separazione dei ruoli per incompatibilità:
  - utenti/ personale che autorizza le utenze e i profili
  - auditor/personale sottoposto ad audit;
  - archivisti/amministratori di sistema;
  - amministratori di sistema/Responsabile della sicurezza;
  - chi svolge un'operazione / chi verifica l'operazione.
- devono essere attuate opportune misure di sicurezza a garanzia di un'adeguata separazione degli ambienti di sviluppo, test e produzione.

4.7 CONTROLLO DEGLI ACCESSI

4.7.1 Obiettivo

L'obiettivo della seguente politica è **garantire l'accesso sicuro alle informazioni conservate**, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti (interni o esterni) che non possiedono i necessari diritti.

4.7.2 Riferimenti esterni:

Per ciò che attiene gli accessi logici ai sistemi informatici gestiti da PAT e l'accesso a tutti gli ulteriori apparati informatici utilizzati da PAT per l'erogazione del servizio di conservazione si fa riferimento al documento "Privacy & Digital Policy Della Provincia Autonoma di Trento", approvato con deliberazione della Giunta provinciale n. 54 del 2019; in particolare si considerano i capitoli:

- 9.2.1 Protezione da accessi logici non autorizzati (Misure di sicurezza relative alle postazioni di lavoro)
- 9.2.2 Protezione da accessi logici non autorizzati a PC non connessi alla rete (Misure di sicurezza relative alle postazioni di lavoro)

Per ciò che attiene l'accesso al Sistema di conservazione SacER, si rimanda alle policy adottate dal Gestore dell'Infrastruttura ed in particolare alla "Politica sulla sicurezza delle informazioni del servizio di conservazione di ParER".

4.7.3 Regole/requisiti:

Il ciclo di vita delle utenze deve essere regolamentato da un'opportuna procedura, dal momento dell'assegnazione dell'utenza, fino alla sua dismissione.

- Personale interno e consulenti – l'accesso alle informazioni da parte di ogni singolo utente (personale PAT, nonché dipendenti di imprese esterne e/o consulenti cui l'accesso è

consentito per l'esecuzione degli specifici obblighi contrattuali) deve essere subordinato ad una procedura di autorizzazione da parte di PAT e limitato alle sole informazioni di cui necessita in funzione del ruolo e delle mansioni assegnate (principio del minimo privilegio);
- Personale esterno (Enti Produttori) - l'accesso alle informazioni da parte degli Utenti degli Enti Produttori deve avvenire secondo precise regole (di accesso e visibilità delle informazioni) condivise da PAT con gli Enti Produttori
- le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo e agli incarichi ricoperti, nel rispetto dei principi di separazione dei ruoli e devono essere sottoposte a revisione periodica, con cadenza almeno annuale. Deve essere in ogni caso prevista la tempestiva modifica/disattivazione dei diritti d'accesso in caso di revisione/sospensione/revoca dei profili autorizzativi assegnati;
- è necessario definire un processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso. Specifiche procedure devono essere definite per l'assegnazione, la gestione e il controllo dei profili associati ad elevati privilegi (es. amministratori di sistema, "superutenti" in genere);
- devono essere definiti standard, procedure e istruzioni per la gestione delle password in conformità alle normative vigenti, con particolare riferimento a quelle in materia di protezione dei dati personali;
- devono essere monitorati e regolarmente verificati, nel rispetto dei limiti imposti dalla vigente normativa sulla protezione dei dati personali, gli accessi da parte degli utenti alla rete, ai servizi di rete, al sistema operativo alle applicazioni e alle informazioni dell'organizzazione;
- deve essere adottata particolare attenzione al tracciamento degli accessi legati alle utenze amministrative, al fine di garantire l'inalterabilità dei log e la loro conservazione secondo le tempistiche previste e per l'espletamento degli obblighi di verifica imposti dalla vigente normativa sulla protezione dei dati personali;
- l'accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati deve essere subordinato al superamento di una procedura di identificazione e autenticazione. La comunicazione e la trasmissione di informazioni all'interno, così come verso l'esterno, deve fondarsi sullo stesso principio.

4.8 CRITTOGRAFIA

4.8.1 Obiettivo

L'obiettivo della seguente politica è quello di **assicurare adeguato livello di protezione ai dati e alle informazioni gestite**.

4.8.2 Riferimenti esterni:

Per ciò che attiene le policy di crittografia del Sistema di conservazione SacER, si rimanda alle policy adottate dal Gestore dell'Infrastruttura ed in particolare alla "Politica sulla sicurezza delle informazioni del servizio di conservazione di ParER".

4.8.3 Regole/requisiti:

- i log degli amministratori di sistema e le password gestite devono essere adeguatamente protette attraverso meccanismi di crittografia;

- i flussi informativi in entrata e in uscita relativi ai servizi di conservazione devono essere protetti mediante idonei protocolli di crittografia (es. HTTPS e FTPS).
- Il processo di conservazione non prevede l'utilizzo della crittografia degli oggetti conservati, in quanto:
  - deve assicurare la conservazione a lungo termine del documento digitale e di conseguenza la piena disponibilità nei confronti non solo dell'ente produttore, ma di tutta la comunità di riferimento (previa verifica dell'autorizzazione all'accesso ai documenti);
  - non deve in alcun modo alterare il documento inviato in conservazione utilizzando tecniche crittografiche proprie.

4.9 SICUREZZA FISICA

4.9.1 Obiettivo

L'obiettivo della seguente politica è quello di **prevenire l'accesso non autorizzato alle sedi e ai locali dell'organizzazion**e e garantire adeguati livelli di sicurezza alle aree e agli asset mediante i quali vengono gestite le informazioni.

4.9.2 Riferimenti esterni:

PAT fa riferimento al sopracitato documento "Privacy & Digital Policy Della Provincia Autonoma di Trento" in materia di sicurezza e privacy, in particolare al Capitolo 9.1 Misure di sicurezza logistiche (Misure di sicurezza relative alle postazioni di lavoro) per quanto concerne l'accesso agli Uffici.

Per ciò che attiene alle modalità di accesso al Datacenter, si rimanda alle policy adottate dal Gestore dell'Infrastruttura ed in particolare alla "Politica sulla sicurezza delle informazioni del servizio di conservazione di ParER".

4.9.3 Regole/requisiti:

Devono essere garantiti:

- delimitazione e opportuna protezione del perimetro fisico relativo ai sistemi di conservazione;
- isolamento/separazione delle aree di carico e scarico;
- adeguati sistemi di controllo e tracciamento degli accessi fisici;
- definizione di una adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni;
- predisposizione di idonei impianti di sicurezza fisica e ambientale;
- predisposizione di un adeguato piano di manutenzione degli impianti di sicurezza fisica e ambientale.

4.10 CAPACITY MANAGEMENT

4.10.1 Obiettivo

L'obiettivo della seguente politica è quello di **garantire una gestione efficace che tenga conto dei necessari livelli di disponibilità e delle performance**.

4.10.2 Riferimenti esterni:

N.A.

4.10.3 Regole/requisiti:

Devono essere attuati i necessari controlli a garanzia del monitoraggio dei volumi gestiti (ad esempio numerosità degli Enti produttori e dei documenti versati), al fine di intervenire con tempismo e assicurare la necessaria disponibilità delle risorse, in coerenza con le esigenze (anche prestazionali) del servizio condivise con gli Enti Produttori.

4.11 GESTIONE MALWARE

4.11.1 Obiettivo

L'obiettivo della seguente politica è quello di **garantire un adeguato livello di sicurezza della piattaforma tecnologica a supporto del servizio (lato client e lato server)**, considerando opportunamente tali aspetti nelle tematiche relative alla gestione del malware.

4.11.2 Riferimenti esterni:

PAT fa riferimento al sopracitato documento "Privacy & Digital Policy Della Provincia Autonoma di Trento" in materia di sicurezza e privacy; in particolare si considera il Capitolo 9.2.4 Protezione dai virus (Misure di sicurezza relative alle postazioni di lavoro), per quanto concerne le postazioni di lavoro.

Per ciò che attiene la gestione del malware sul Sistema di conservazione SacER, si rimanda alle policy adottate dal Gestore dell'Infrastruttura ed in particolare alla "Politica sulla sicurezza delle informazioni del servizio di conservazione di ParER".

4.11.3 Regole/requisiti:

Devono essere definite opportune politiche di protezione delle postazioni di lavoro e dei server dalla contaminazione di malware, che prevedano:

- identificazione delle postazioni e dei sistemi operativi target, in base alle esigenze operative e alla diffusione degli attacchi;
- selezione di opportune tecnologie anti-malware;
- definizione di modalità di installazione delle tecnologie anti-malware;
- definizione delle modalità di aggiornamento e verifica della corretta configurazione;
- definizione di meccanismi di notifica early-warning.

4.12 BACKUP

4.12.1 Obiettivo

L'obiettivo della seguente politica è quello di considerare opportunamente, nella fase di realizzazione ed esercizio, gli aspetti di sicurezza relativamente all'adozione di **procedure di backup e ripristino dei dati**.

4.12.2 Riferimenti esterni:

Per il backup della documentazione, PAT fa riferimento alle indicazioni presenti nella Delibera n. 54 "Privacy & Digital Policy Della Provincia Autonoma di Trento" adottata in materia di sicurezza e privacy dalla Provincia autonoma di Trento; in particolare si considera il Capitolo 6.3.4 Protezione dal rischio di perdita accidentale dei dati (6. Misure di sicurezza relative ai server) e il Capitolo 9.4.2.4 Protezione dal rischio di perdita accidentale dei dati (9. Misure di sicurezza relative alle postazioni di lavoro).

Per ciò che attiene la gestione del backup del Sistema di conservazione SacER, si rimanda alle policy adottate dal Gestore dell'Infrastruttura ed in particolare alla "Politica sulla sicurezza delle informazioni del servizio di conservazione di ParER".

4.12.3 Regole/requisiti:

Le seguenti attività sono svolte dall'amministratore di sistema (ParER), titolare dell'infrastruttura tecnologica.

- devono essere garantiti adeguate misure e strumenti di backup in funzione dell'importanza dei sistemi e dei dati in essi contenuti in modo da assicurare che i dati, le configurazioni e i software possano essere ripristinati successivamente ad un malfunzionamento o un crash di sistema;
- le procedure di backup/rispristino dei dati devono tener conto delle peculiarità del servizio di conservazione (i dati in conservazione non devono essere più modificati), pertanto è da preferire la modalità incrementale di backup. Per gli altri dati, invece, è possibile fare riferimento alle politiche della Provincia;
- i supporti di backup devono essere conservati in una location differente rispetto a quella in cui sono conservati i dati originari, ad una sufficiente distanza dalla location originaria e deve essere garantito un adeguato livello di protezione fisica.
- il processo di back up e restore dei dati deve essere periodicamente testato, e gli esisti delle verifiche opportunamente documentati.

4.13 Monitoraggio e Gestione dei Log

4.13.1 Obiettivo

L'obiettivo della seguente politica è quello di **garantire i livelli di sicurezza necessari nella gestione e monitoraggio degli eventi e delle attività relative alla Sicurezza Informatica** sul sistema di conservazione.

4.13.2 Riferimenti esterni:

Per quanto concerne i log relativi al traffico internet del personale, PAT fa riferimento alla Delibera n.54 "Privacy & Digital Policy Della Provincia Autonoma di Trento", adottata in materia sicurezza e privacy; in particolare si considerano i Capitoli:

- 11.4 Conservazione dei log (11. Misure di sicurezza relative a internet);
- 12.4.3.2 Verifiche puntuali a posteriori (12. Verifiche di sicurezza);
- 12.4.3.3 Verifiche periodiche (12. Verifiche di sicurezza).

Per ciò che attiene la gestione dei log del Sistema di conservazione SacER, si rimanda alle policy adottate da Gestore dell'Infrastruttura ed in particolare alla "Politica sulla sicurezza delle informazioni del servizio di conservazione di ParER".

4.13.3 Regole/requisiti:

Le seguenti attività sono svolte dall'amministratore di sistema (ParER), titolare dell'infrastruttura tecnologica.

- devono essere loggati gli eventi e le attività ogniqualvolta questi coinvolgano il sistema di conservazione; inoltre deve essere possibile associare i log all'utente che ha effettuato le attività;
- il contenuto dei log può variare a seconda dei sistemi considerati e in funzione delle limitazioni tecniche presenti;
- devono essere soggette a log le seguenti attività che vanno monitorate con regolarità:
    - tentativi di accesso (falliti e riusciti) ai sistemi più critici;
    - utenti creati o disabilitati dai sistemi;
    - assegnazione e utilizzo di particolari privilegi a sistema;
    - utilizzo di utenze di amministratore;
- devono essere ben identificate le fonti dei log (componenti infrastrutturali, applicative e le attività da monitorare);
- i dati di log raccolti devono essere adeguatamente protetti da accessi non autorizzati e preservati nella loro integrità;
- i dati di log vanno conservati per il tempo minimo necessario a rispondere alla finalità per la quale sono stati raccolti e comunque nel rispetto di quanto previsto dalle politiche del Gestore dell'Infrastruttura;
- i dati di log vanno revisionati con cadenza periodica, allo scopo di identificare eventuali anomalie e porvi rimedio.

4.14 COMPLIANCE

4.14.1 Obiettivo

L'obiettivo della seguente politica è quello di **garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni**, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni reputazionali.

4.14.2 Riferimenti esterni:

N.A.

4.14.3 Regole/requisiti:

Deve essere garantito il rispetto dei requisiti in merito a:

- disposizione di legge applicabili in merito alla protezione dei dati personali e relativi Provvedimenti del garante, in riferimento ai dati trattati sia in qualità di titolare del trattamento, sia in qualità di responsabile del trattamento nell'ambito del servizio di conservazione;
- disposizioni di legge in merito alla tutela dei beni culturali;
- normativa sulla conservazione;

- norma ISO/IEC 27001:2013;
- i requisiti richiesti da AgID per la qualificazione dei soggetti che svolgono attività di conservazione dei documenti;
- obblighi contrattuali legati al servizio, con particolare riferimento agli obblighi in materia di protezione dei dati.

4.15 GESTIONE DEGLI INCIDENTI

4.15.1 Obiettivo

L'obiettivo della seguente politica è quello di **garantire che gli incidenti aventi ripercussioni sul Servizio di Conservazione e sulla sicurezza delle informazioni siano tempestivamente riconosciuti e correttamente gestiti** attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto su PAT e sugli Enti Produttori.
Per incidente di sicurezza delle informazioni (di seguito "incidente") si intende un evento accidentale o un'azione deliberata potenzialmente in grado di compromettere almeno uno dei requisiti di sicurezza del Servizio di Conservazione.

4.15.2 Riferimenti esterni:

Per quanto concerne la gestione di incidenti di sicurezza, PAT fa riferimento alla Delibera n.54 "Privacy & Digital Policy Della Provincia Autonoma di Trento", adottata in materia sicurezza e privacy; in particolare si considerano i Capitoli:

- 12.4.3.2 Verifiche puntuali a posteriori (12. Verifiche di sicurezza);
- 2) Modello di rapporto sull'incidente di sicurezza (Appendice).

Per ciò che attiene la gestione degli incidenti relativi del Sistema di conservazione SacER, si rimanda alle policy adottate da Gestore dell'Infrastruttura ed in particolare alla "Politica sulla sicurezza delle informazioni del servizio di conservazione di ParER".

4.15.3 Regole/requisiti:

- tutti i dipendenti e i collaboratori sono tenuti a rilevare e notificare a chi di competenza e secondo adeguate procedure eventuali eventi rilevanti per la sicurezza delle informazioni;
- gli incidenti rilevati devono essere comunicati a tutti i soggetti coinvolti e, ove prescritto dalla legge o dalla normativa regolamentare, alle autorità e agli enti competenti, in coordinamento con la Provincia e nel rispetto delle procedure da essa previste (es. notifiche di Data Breach);
- gli eventi/incidenti che possano avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni, potenziali e non, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure condivise con tutti i soggetti interessati (a partire dagli Enti Produttori);
- deve esistere un sistema di registrazione e classificazione degli incidenti per effettuare analisi volte al miglioramento dei livelli di sicurezza delle informazioni coerentemente con le reali problematiche riscontrate;
- gli audit log inerenti alle attività degli utenti, degli amministratori di sistema e degli operatori di sistema e agli eventi che possono compromettere la sicurezza delle risorse informative devono essere tracciati, registrati e conservati per un periodo di tempo ritenuto

idoneo (anche in conformità alle normative vigenti) ai fini della ricostruzione degli incidenti e a supporto di future attività di accertamento di comportamenti illeciti.

4.16 CONTINUITÀ OPERATIVA

4.16.1 Obiettivo

L'obiettivo della seguente politica è quello di **garantire la continuità operativa del servizio di conservazione** e l'eventuale ripristino tempestivo dei servizi erogati nel momento in cui siano stati colpiti da eventi anomali di una certa gravità, riducendo le conseguenze di tali eventi sia all'interno che all'esterno del contesto dell'organizzazione.

4.16.2 Riferimenti esterni:

Per ciò che attiene la Continuità Operativa del Sistema di conservazione SacER, si rimanda alle policy adottate da Gestore dell'Infrastruttura ed in particolare alla "Politica sulla sicurezza delle informazioni del servizio di conservazione di ParER".

4.16.3 Regole/requisiti:

- deve essere sviluppato un piano di continuità operativa che si basi su un'analisi dei rischi e un'analisi degli impatti che tenga conto delle reali necessità del servizio e delle aspettative degli Enti Produttori;
- il piano deve essere opportunamente comunicato e aggiornato;
- il piano deve essere periodicamente sottoposto a test di verifica;
- devono essere correttamente mantenuti i rapporti con tutti i soggetti interessati in caso di disastro;
- anche in situazione di crisi e disastro, devono essere mantenuti requisiti di sicurezza delle informazioni trattate.

4.17 VERIFICHE DI SICUREZZA E PATCHING

4.17.1 Obiettivo

L'obiettivo della seguente politica è quello di **garantire la rilevazione di vulnerabilità potenziali dei sistemi informativi** al fine di assicurare la sicurezza e la disponibilità dei servizi e delle relative informazioni.

4.17.2 Riferimenti esterni:

PAT fa riferimento alla Delibera n.54 "Privacy & Digital Policy Della Provincia Autonoma di Trento", adottata in materia di sicurezza e privacy; in particolare si considera il Capitolo 12. Verifiche di sicurezza.

Per ciò che attiene le attività di Verifica e di Patching sul Sistema di conservazione SacER, si rimanda alle policy adottate dal Gestore dell'Infrastruttura ed in particolare alla "Politica sulla sicurezza delle informazioni del servizio di conservazione di ParER".

4.17.3 Regole/requisiti:

- Devono essere pianificate attività periodiche orientate alla verifica di conformità e efficacia del sistema di gestione della sicurezza delle informazioni, ad esempio rivolte a:
  - processi di pianificazione, attuazione, controllo e miglioramento del sistema;
  - attuazione ed efficacia del sistema dei controlli organizzativi;
  - attuazione ed efficacia del sistema dei controlli tecnologici, anche attraverso attività di vulnerability assessment e/o penetration test.
- Devono essere pianificate ed effettuate attività periodiche di patching sui Sistemi e sulle PDL, al fine di garantire la risoluzione delle vulnerabilità di sicurezza riscontrate da Vendor.

4.18 SICUREZZA DELLE COMUNICAZIONI

4.18.1 Obiettivo

L'obiettivo della seguente politica è quello di garantire che siano opportunamente considerati gli aspetti di sicurezza nelle tematiche relative alla sicurezza delle comunicazioni (Network security: segregazione delle reti, monitoraggio dei gateway (firewall)).

4.18.2 Riferimenti esterni:

PAT fa riferimento:

- alla Delibera n.54 "Privacy & Digital Policy Della Provincia Autonoma di Trento", adottata in materia di sicurezza e privacy; in particolare si considera il Capitolo 11. Misure di sicurezza relative a internet;
- al Disciplinare per l'utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche.

Per ciò che attiene la sicurezza delle comunicazioni specifiche del Sistema di conservazione SacER, si rimanda alle policy adottate dal Gestore dell'Infrastruttura ed in particolare alla "Politica sulla sicurezza delle informazioni del servizio di conservazione di ParER".

4.18.3 Regole/requisiti:

- Tutti i flussi contenenti pacchetti informativi in entrata e in uscita nell'esercizio dei servizi di conservazione devono essere protetti mediante opportuni protocolli di crittografia (HTTPS e FTPS) o veicolati attraverso canali di posta certificata (PEC).
- Ove possibile, i flussi di traffico originati dall'utenza del servizio (interna ed esterna) sono separati da quelli legati alle attività di amministrazione e gestione (i.e. reti differenziate).

4.19 RELAZIONI CON AUTORITÀ ESTERNE E GRUPPI SPECIALISTICI

4.19.1 Obiettivo

L'obiettivo della seguente politica è quello di **garantire che siano stati identificati i referenti per mantenere le necessarie relazioni con le autorità esterne**.

4.19.2 Riferimenti esterni:

N.A.

4.19.3 Regole/requisiti:

- Devono essere identificate e assegnate le responsabilità per i contatti e le comunicazioni relative a questioni inerenti la sicurezza delle informazioni del servizio di conservazione nei confronti delle diverse autorità.

In particolare,

  - il Responsabile Ufficio Beni archivistici, librari e Archivio provinciale è responsabile per le comunicazioni con:
    - AgID;
    - la Soprintendenza archivistica;
    - la Magistratura;
    - l'Ente di certificazione;
  - il Responsabile della Sicurezza delle Informazioni è responsabile per le comunicazioni con:
    - gruppi specialistici in tema security;
    - il Garante per la protezione dei dati personali.

- Devono essere opportunamente individuati i flussi di comunicazione verso l'interno e verso l'esterno, rilevanti per la sicurezza delle informazioni.

In particolare:

  - comunicazioni legate alle funzioni di vigilanza (AgID, Soprintendenza archivistica);
  - comunicazioni legate ad eventi che hanno impatto sui requisiti di disponibilità, integrità e riservatezza.

4.20 TELELAVORO E ATTIVITÀ SVOLTE AL DI FUORI DELLA SEDE PAT

4.20.1 Obiettivo

L'obiettivo della seguente politica è quello di garantire che, sia nel caso di telelavoro sia di attività svolte al di fuori della sede PAT, siano rispettati gli stessi requisiti di sicurezza garantiti dall'utilizzo delle postazioni di lavoro interne alla sede di PAT.

4.20.2 Riferimenti esterni:

PAT fa riferimento al:

- Delibera n.54 "Privacy & Digital Policy Della Provincia Autonoma di Trento", adottata in materia di sicurezza e privacy; in particolare si considera il Capitolo 9.6.1 Uso Corretto delle dotazioni informatiche.
- Disciplinare per l'utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche.

4.20.3 Regole/requisiti:

- Nel caso di personale che svolge delle attività lavorative relative al Servizio di conservazione al di fuori della sede PAT, è necessario rispettare quanto indicato nella presente "Politica sulla sicurezza delle informazioni del sistema di conservazione" e nei

seguenti documenti: "Privacy & Digital Policy Della Provincia Autonoma di Trento", "Politica sulla sicurezza delle informazioni del sistema di conservazione" e "TelePAT 2.0 Modalità di applicazione della Normativa contrattuale in materia di telelavoro nella Provincia Autonoma di Trento".

- Le casistiche del lavoro al di fuori della sede PAT sono:
  - telelavoro domiciliare e presso telecentro;
  - telelavoro mobile (solo per direttori e dirigenti);
  - lavoro agile.

4.21 GESTIONE DEI CAMBIAMENTI

4.21.1 Obiettivo

L'obiettivo della seguente politica è quello di garantire che i cambiamenti che coinvolgono i servizi di PAT siano opportunamente gestiti al fine di evitare impatti negativi sulla sicurezza delle informazioni.

4.21.2 Riferimenti esterni:

N.A.

4.21.3 Regole/requisiti:

Di seguito si elencano regole e principi applicabili:

- I cambiamenti devono essere opportunamente comunicati ai soggetti interessati;
- Nel caso di cambiamenti significativi, questi devono essere gestiti tramite progetti specifici, documentati a cura di un Responsabile definito, secondo l'ambito di competenza;
- tutti i cambiamenti, che hanno un impatto sugli utenti del Servizio di conservazione, devono essere comunicati tramite opportuni canali.

5 RUOLI E RESPONSABILITÀ

Per attuare una politica di Sicurezza delle Informazioni efficiente e efficace è necessario stabilire una struttura organizzativa che sia in grado di definire, implementare e controllare l'applicazione della Politica stessa attraverso:

- la definizione degli obiettivi e delle finalità delle politiche di sicurezza identificate;
- la realizzazione del sistema di gestione della sicurezza delle informazioni, assicurandosi che tutti gli aspetti rilevanti per la Sicurezza delle informazioni si realizzino in conformità alle necessità del servizio di conservazione;
- la definizione di misure coerenti e adeguate al valore del patrimonio da proteggere e all'obiettivo del monitoraggio dell'efficacia del sistema per la sicurezza delle informazioni.

Per questo motivo, a supporto della gestione della sicurezza delle informazioni, PAT si è dotato di un'adeguata struttura organizzativa, in grado di definire le procedure di gestione della Sicurezza delle informazioni, di implementare tali procedure e di mantenere le misure di protezione delle informazioni, nonché di adempiere a tutti i vincoli imposti dalle normative vigenti.

6 VIOLAZIONI

Qualunque violazione a queste norme deve essere individuata e gestita. Il personale che contravviene alle politiche definite in questo documento potrà essere sanzionato secondo quando definito nel contratto di lavoro con il dipendente.

7 CICLO DI REVISIONE

Il presente documento è di proprietà di PAT, ed è compito di PAT provvedere all'aggiornamento del medesimo ogni qualvolta vengano riviste le strategie dell'organizzazione e gli standard/normative di riferimento.

Il ciclo di aggiornamento viene incluso in un ciclo di Management review del SGSI al quale il Servizio di Conservazione si riferisce. PAT gestisce e assicura il Riesame periodico da parte della Direzione del SGSI stesso, effettuandone una valutazione globale sullo stato e sull'efficacia.

L'obiettivo del Management review è quello di:

- assicurare l'idoneità, l'adeguatezza e l'efficacia nel tempo del SGSI in termini di processi, organizzazione e risorse;
- verificare il livello di sicurezza raggiunto;
- rivedere le politiche di sicurezza.

Il Riesame deve tenere conto di variazioni del quadro legislativo nazionale e del quadro normativo interno all'organizzazione di PAT, di variazioni organizzative interne, di variazioni delle informazioni trattate in termini di numerosità e/o tipologia, delle infrastrutture tecnologiche e dei processi operativi compresi nel perimetro, dell'individuazione di nuove minacce e di variazioni degli obiettivi di sicurezza. Viene effettuato con frequenza almeno annuale, che può diventare maggiore in base alle necessità o a seguito di particolari condizioni rilevate nell'ambito di verifiche ispettive / monitoraggi / analisi di incidenti di sicurezza.

Elementi di input al riesame del SGSI sono infatti, tra gli altri, i risultati dei precedenti riesami, i risultati raccolti in sede di verifiche tecniche, ispettive e audit, sia interni che esterni, lo stato delle azioni correttive individuate nel piano di trattamento del rischio.

A valle del Riesame periodico almeno annuale, il responsabile del Servizio identifica i possibili miglioramenti applicabili al sistema e i nuovi obiettivi per la sicurezza delle informazioni, comunicati successivamente a tutti i soggetti interessati; vengono dunque pianificate le modalità con cui procedere, le azioni necessarie al raggiungimento degli obiettivi e le risorse da impiegare a tale scopo.