ALLEGATO N. 1

PIANO DI SICUREZZA RELATIVO ALLA FORMAZIONE, ALLA GESTIONE, ALLA TRASMISSIONE, ALL'INTERSCAMBIO, ALL'ACCESSO, ALLA CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Premessa

Il presente Piano di Sicurezza, adottato ai sensi delle Linee Guida Agid, garantisce che:

- i documenti, e le relative informazioni, trattati dal Consorzio Boschi Carnici siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

A tali fini si individua i requisiti minimi di sicurezza dei sistemi di protocollo informatico cui il presente piano si conforma.
Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi cui sono esposti i dati (personali e non), e/o i documenti trattati, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno del Consorzio Boschi Carnici;
- le modalità di accesso al Sistema di Gestione Informatica dei Documenti;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui al disciplinare tecnico richiamato nell'allegato b) del decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali, in caso di trattamento di dati personali;
- la formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Tale Piano di Sicurezza è soggetto a revisione con cadenza almeno biennale; a seguito di particolari esigenze, determinate da sopravvenienze normative o evoluzioni tecnologiche, potrà essere modificato anticipatamente.

Elementi di rischio cui sono soggetti i documenti informatici e i dati contenuti nel Sistema di Gestione Informatica dei Documenti

I principali elementi di rischio cui sono soggetti i documenti informatici e i dati trattati con l'ausilio delle tecnologie informatiche sono essenzialmente riconducibili alle seguenti tipologie:

- accesso non autorizzato, sia esso inteso come accesso al Sistema di Gestione Informatica dei Documenti (SGID) o come accesso ai documenti, dati e unità archivistiche in esso contenuti;
- cancellazione o manomissione dei documenti e dei dati, includendo a tale proposito tutti i dati presenti sul Sistema di Gestione Informatica dei Documenti;
- perdita dei documenti e dei dati contenuti nel Sistema;
- trattamento illecito, eccedente rispetto allo scopo o comunque non in linea con la normativa vigente, dei dati personali.

Per prevenire tali rischi e le conseguenze da essi derivanti, il Consorzio Boschi Carnici adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

Sicurezza della rete di accesso al servizio

Misure adottate per la protezione della rete Consorzio Boschi Carnici

Firewall e VPN
La Lan della sede Consorzio Boschi Carnici deve essere considerata come una rete più che sufficientemente informatizzata e sicura. Vi è un sistema firewall come protezione perimetrale relativo alla messa in sicurezza delle comunicazioni Untrusted che avvengono tra l'esterno della rete (tipicamente Internet/Extranet) ed il resto dell'infrastruttura. Tra il perimetro esterno dell'infrastruttura e quello interno si è creata una zona filtro, denominata "**DMZ**".
Le contromisure necessarie per proteggere le comunicazioni che avvengono all'interno dell'organizzazione sono attuate tramite l'adozione di un dominio di Active Directory e a un sistema di Antivirus.
Da un punto di vista generale, qualsiasi accesso esterno alla rete aziendale ma in particolare al protocollo, può costituire una minaccia per l'organizzazione. Tuttavia la necessità di avere costantemente a disposizione i dati aziendali, anche quando non è possibile fisicamente accedere al sistema informativo dall'interno, impone l'utilizzo di tecnologie in grado di fornire un accesso diretto ai sistemi interni con una connessione telefonica o similare, da qualsiasi punto del mondo ed indipendentemente dall'orario locale. Per far fronte a tale necessità si è strutturato un sistema che prevede l'inserimento all'interno della **DMZ** di un **reverse proxi** come ulteriore protezione dal WEB per permettere la pubblicazione su internet del SGID.

Storage ad alta affidabilità: il sistema prevede porte multiple di collegamento tra i server e la SAN, controller e schede di rete ridondati, i collegamenti con gli shelf di espansione sono realizzati con fibre ottiche e i dischi della SAN configurati con livello di RAID 10;

cluster: composto da tre SERVER fisici in replica, nel caso un server dovesse andare in fault, in modo automatico tutti i server virtuali vengono spostati sul server fisico che è rimasto attivo (live-migration).

Alta disponibilità: i tre Server sono configurati in cluster connessi ad una risorsa comune (SAN) con i dati condivisi in una storage con la possibilità che permette di esportare una o più LUN verso diversi server.

Accesso non autorizzato a computer e reti informatiche
L'accesso a computer e reti informatiche è normalmente autorizzato solo per i soggetti che superano un processo di autenticazione dell'utente, inteso come il riconoscimento dell'identità dichiarata.

Accesso al Sistema di Gestione Informatica dei Documenti e ai documenti e dati in esso contenuti da parte di utenti interni all'AOO

L'accesso al Sistema di Gestione Informatica dei Documenti, da parte degli utenti interni all'AOO, avviene attraverso l'utilizzo di credenziali di autenticazione. L'accesso ai documenti e ai dati presenti sul Sistema è definito in base al livello di riservatezza degli stessi.
Le credenziali di autenticazione consistono in un codice (User-Id), per l'identificazione dell'incaricato, associato ad una parola chiave riservata (Password), conosciuta solamente dal medesimo; tali credenziali vengono verificate in tempo reale da un apposito sistema di identificazione/autenticazione, il quale consente l'accesso ai soggetti abilitati e traccia tutti gli accessi di ciascun utente, memorizzando, ai fini di controllo, l'User-Id corrispondente, ma non la Password dello stesso.

Agli incaricati è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della Password; quest'ultima è composta da almeno otto caratteri, tra cui almeno un numero e un carattere speciale e non contiene riferimenti agevolmente riconducibili al titolare. La Password deve essere modificata dall'incaricato al suo primo utilizzo e, successivamente, con cadenza trimestrale.

L'User-Id non può essere assegnato a nessun altro incaricato per nessuna motivazione. Le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; tali credenziali sono altresì disattivate anche nel caso di perdita della qualità (intesa come efficacia sulla sicurezza) che consente all'incaricato l'accesso ai dati personali.

Il Responsabile della sicurezza informatica del Consorzio Boschi Carnici non è in grado di conoscere la Password dell'utente; qualora l'utente medesimo dimenticasse la propria Password si procederà all'assegnazione di una nuova chiave di accesso.

Accesso al trattamento di dati personali sensibili o giudiziari e politiche di sicurezza espressamente previste

L'accesso ai documenti contenenti dati personali, sensibili o giudiziari e ai dati medesimi avviene per mezzo dell'individuazione di specifici profili di autorizzazione, stabiliti sulla base del livello di riservatezza di ciascun documento, fascicolo o sottofascicolo, secondo quanto stabilito dall'art. 65 del presente Manuale; tali profili, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento.

Periodicamente, e comunque con cadenza almeno annuale, deve essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Gli incaricati del trattamento di dati personali, sensibili o giudiziari non devono lasciare incustodita e accessibile la propria postazione di lavoro durante il trattamento degli stessi.

Trattamento dei dati personali, sensibili o giudiziari senza l'ausilio di strumenti elettronici

Ai fini del trattamento dei dati personali, sensibili o giudiziari, devono essere impartite agli incaricati istruzioni scritte da parte del Responsabile per il trattamento dei dati personali, relative alle modalità delle operazioni, del controllo e della custodia di atti e documenti. Analogamente al trattamento dei medesimi dati svolto per mezzo di strumenti elettronici, sarà verificato il sussistere delle condizioni per l'accesso e il trattamento dei suddetti dati, da parte di ciascun utente o gruppo di utenti, con cadenza almeno annuale.

I suddetti documenti, sono controllati e custoditi dagli incaricati del trattamento per tutto il tempo di svolgimento dei relativi compiti; nell'arco di tale periodo gli incaricati medesimi si assicureranno che a tali documenti non accedano persone prive di autorizzazione.

L'accesso agli archivi contenenti dati sensibili o giudiziari è consentito solo previa autorizzazione; le persone ammesse sono identificate e registrate.

Formazione dei documenti

I documenti dell'AOO sono prodotti utilizzando i formati previsti dall'allegato 2 delle Linee Guida Agid.
L'apposizione della firma digitale, volta a garantire l'attribuzione certa della titolarità del documento e la sua integrità, avviene previa conversione in un formato, tra quelli previsti dal suddetto allegato, che garantisca la leggibilità, l'interscambiabilità, la non alterabilità, l'immutabilità nel tempo del contenuto e della struttura del documento medesimo (ad esempio il formato PDF/A); l'acquisizione mediante scansione dei documenti analogici avverrà in uno dei formati avente le medesime caratteristiche.

L'apposizione delle varie tipologie di sottoscrizioni elettroniche, l'apposizione della firma digitale, nonché la validazione temporale del documento sottoscritto digitalmente deve avvenire in conformità a quanto sancito dell'art. 20 c. 1 del D.Lgs. 82/2005 (CAD), come modificato dal D.Lgs. n. 179/2016 .
La sottoscrizione del documento con firma digitale deve avvenire prima dell'effettuazione della registrazione di protocollo.

Sicurezza delle registrazioni di protocollo

L'accesso al registro di protocollo al fine di effettuare le registrazioni o di apportare modifiche è consentito soltanto al personale abilitato alla protocollazione.
L'accesso in consultazione al registro di protocollo è consentito sulla base dell'organizzazione del Consorzio Boschi Carnici: di norma, ciascun operatore è abilitato ad accedere ai documenti e ai dati di protocollo dei documenti dell'Amministrazione ad eccezione di quelli "riservati" se non gli competono.
Ogni registrazione di protocollo viene memorizzata dal Sistema di Gestione Informatica dei Documenti, unitamente all'identificativo univoco dell'autore che l'ha eseguita insieme alla data e l'ora della stessa.
Eventuali modifiche, autorizzate, vengono registrate per mezzo di log di sistema che mantengano traccia dell'autore, della modifica effettuata, nonché della data e dell'ora; il Sistema mantiene leggibile la precedente versione dei dati di protocollo, permettendo, in tal modo, la completa ricostruzione cronologica di ogni registrazione.

Il Sistema non consente la modifica del numero e della data di protocollo; in tal caso l'unica possibile modifica è l'annullamento della registrazione stessa di cui, analogamente al caso precedente, il Sistema manterrà traccia. L'annullamento di una registrazione di protocollo deve sempre essere accompagnato da autorizzazione scritta del Responsabile della gestione documentale e il SGID deve recare, in corrispondenza della registrazione annullata, gli estremi del provvedimento di autorizzazione.

Gestione dei documenti e sicurezza logica del Sistema

I documenti informatici, una volta registrati sul Sistema di Gestione Informatica dei Documenti, risultano immodificabili e non eliminabili; l'accesso ad essi, da parte degli utenti interni all'AOO, avviene soltanto attraverso il Sistema medesimo, previa la suddetta procedura di identificazione informatica e nel rispetto dei profili di autorizzazione di ciascun utente.
Il Sistema consente l'effettuazione di qualsiasi operazione su di esso o sui dati, documenti, fascicoli e aggregazioni documentali in esso contenuti, esclusivamente agli utenti abilitati per lo svolgimento di ciascuna attività; il Sistema effettua, inoltre, il tracciamento di qualsiasi evento di modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione; tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.
Il Sistema e tutti i documenti e/o dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici dannosi in quanto il Consorzio Boschi Carnici si impegna a rendere ragionevolmente sicuri gli accessi al Sistema e tutti i documenti e dati in esso contenuti

tramite collegamento criptato, inoltre si impegna ad aprire le porte in uscita (LAN to WAN) del firewall esclusivamente verso gli indirizzi preventivamente individuati dal titolare del trattamento o dal responsabile all'uopo incaricato.

I sistemi di sicurezza sopra elencati sono gestiti giornalmente da personale tecnico del Consorzio Boschi Carnici e ottemperano al D.Lgs. 196/03 e ss.mm.ii.
Ai fini di ridurre la vulnerabilità dei sistemi informativi, il sistema operativo utilizzato dall'AOO e il Sistema di Gestione Informatica dei Documenti, vengono costantemente tenuti aggiornati, per mezzo dell'istallazione degli aggiornamenti periodici che i fornitori rendono disponibili.

Backup e ripristino dell'accesso ai dati

Come previsto dalle linee guida Agid, il sistema di gestione Protocollo è collocato esternamente su datacenter presso Insiel Spa.
Il Backup dei dati contenuti nel Sistema di Gestione Informatica dei Documenti avviene giornalmente a cura di Insiel Spa.

Il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici è a carico di Insiel Spa che provvede entro 24/36 ore lavorative in caso di generico malfunzionamento, ed entro 72 ore lavorative in caso di disastro.

Trasmissione e interscambio dei documenti

La trasmissione e l'interscambio di documenti e fascicoli informatici all'interno del Consorzio Boschi Carnici avviene esclusivamente per mezzo del Sistema di Gestione Informatica dei Documenti; nessun'altra modalità è consentita, al fine di evitare la dispersione e la circolazione incontrollata di documenti e dati.
La trasmissione di documenti informatici al di fuori del Consorzio Boschi Carnici avviene tramite PEC o mediante i meccanismi dell'interoperabilità e della cooperazione applicativa di cui al Sistema Pubblico di Connettività, utilizzando le informazioni contenute nella segnatura di protocollo.
Le informazioni relative alla segnatura di protocollo sono strutturate in un file conforme alle specifiche XML, compatibile con un file XML Schema e/o DTD, secondo quanto previsto dall'allegato 6 delle Linee Guida Agid.

Conservazione dei documenti

I documenti registrati sul SGID sono conformi ai requisiti e contengono i metadati previsti ai fini della conservazione permanente. Il trasferimento in conservazione avverrà mediante la produzione di pacchetti di versamento, basati su uno schema XML conforme a quanto previsto nel Manuale di conservazione.

Accesso di Utenti esterni al Sistema

L'esercizio del diritto di accesso da parte di utenti esterni al Sistema viene effettuato nel rispetto di quanto sancito dalla legge 241/90 e del D. Lgs. 196/03.
Qualora l'utente esterno decida di esercitare il proprio diritto di accesso presentando apposita richiesta, l'ufficio di competenza gli metterà a disposizione soltanto dati o notizie che riguardino il soggetto interessato adottando gli opportuni accorgimenti.

Piani formativi del personale

In conformità a quanto disposto dall'art. 13 del D.lgs. 82/2005, ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, l'Ente predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo del Sistema di Gestione Informatica dei Documenti;
- fascicolazione dei documenti informatici;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative alla gestione documentale;
- legislazione in materia di protezione dei dati personali;
- aggiornamento sui temi suddetti.

Monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza

L'amministratore di Sistema controlla periodicamente i log di sistema e li mantiene per 6 mesi, al fine di verificare eventuali violazioni del Sistema.
Il Responsabile della gestione documentale dell'Amministrazione effettua periodiche verifiche sul corretto funzionamento del Sistema di Gestione Informatica dei Documenti, valutando a tal fine, anche per mezzo di controlli a campione, il corretto svolgimento delle operazioni inerenti la gestione documentale.