AMBITO TERRITORIALE OTTIMALE
CITTÀ METROPOLITANA DI MILANO

UFFICIO D'AMBITO DELLA CITTÀ METROPOLITANA DI MILANO - AZIENDA SPECIALE
VIALE PICENO 60 - 20129 MILANO
TELEFONO: 02 7740 1 (CENTRALINO)

Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi dell'Ufficio d'Ambito della Città Metropolitana di Milano – Azienda Speciale

Allegato n. 13

Piano per la sicurezza informatica

PIANO di SICUREZZA INFORMATICA

Riferimento al R. UE 679/2016

AMBITO DELLA CITTA' METROPOLITANA DI MILANO

Anno 2021

01	28 Giugno 2021	Prima emissione del Piano Sicurezza	Direttore Generale	Titolare del Trattamento
Rev.	Data	Causale	Preparato da	Titolare Trattamento dei Dati

Indice

LF-1. **PREMESSA**

L'ufficio d'Ambito della Città metropolitana di Milano (dora in poi anche Azienda Speciale -ATO), in qualità di soggetto pubblico, ha predisposto il presente Piano delle Sicurezza del Sistema Informativo (nel seguito denominato più semplicemente PSSI) che definisce le policy di sicurezza inerente il sistema di gestione delle informazioni dell'Azienda.
Il piano della sicurezza identifica:

- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- gli asset/strumenti utilizzati per il trattamento delle banche dati;
- Il Registro dei trattamenti;
- l'analisi dei rischi in materia di trattamento die dati (Privacy Impact Assessment;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- le attività di formazione relative agli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

Allo scopo di adeguarsi al dettato del Regolamento, L'azienda Speciale ha provveduto ad effettuare un censimento generale delle banche dati sia cartacee che informatizzate contenenti dati personali, distribuite in tutte le sedi del suddetto Ente.

LF-2. **CAMPO DI APPLICAZIONE**

Il presente documento sulla Sicurezza del Sistema Informativo, si applica a tutti i dati trattati direttamente dal Titolare o, per incarico dello stesso, gestiti all'esterno presso terzi, sia con strumenti elettronici o comunque automatizzati che con altri strumenti e supporti, anche non elettronici.
Esso è l'atto conclusivo di una serie di verifiche sullo stato della "sicurezza informatica" nell'Azienda Speciale. La presente procedura si applica alle sedi sotto identificate:

Denominazione Sede	Indirizzo
Ufficio d'Ambito della Città Metropolitana di Milano	Viale Piceno, 60 Milano 20129 – MI
Sede secondaria – Archivio di deposito – Bruco Service Srl	Via Ungaretti n. 35 – Opera (MI)

LF-3. **CONCETTI, ABBREVIAZIONI, DEFINIZIONI**

SW: software

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Dati Personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dati Personali Particolari (dati sensibili): dati idonei a rivelare l'origine razziale etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati Giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3 comma 1, lettere da a) ad o) e da r) ad u) del DPR 14 novembre 2002, n 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Titolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati Membri

Responsabile ai sensi dell'Art 28 del GDPR: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile

Interessato: persona fisica, l'ente o l'associazione cui si riferiscono i dati personali.

archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Rischio: con il termine di rischio si identifica l'esposizione alla possibilità di ottenere un guadagno o una perdita economica o finanziaria, di sopportare un danno fisico o un ritardo, come conseguenza dell'incertezza associata al perseguimento di un determinato corso d'azione

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Pseudonimizzazione: il trattamento di dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

diffusione, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

reti di comunicazione elettronica, i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

"posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Vengono di seguito elencate ulteriori definizioni, utilizzate all'interno del presente documento, che possono risultare utili al fine di una maggiore comprensione dello stesso:

"amministratore di rete", soggetto cui è conferito il compito di sovrintendere alla gestione delle risorse fisiche e logiche di una o più reti locali (LAN);

"S.I.A.", sistema informatico aziendale; l'insieme delle strutture fisiche e logiche (hardware e software) che consentono il trattamento dei dati attraverso apparecchiature informatiche;

"dominio", insieme di utenti e gruppi di utenti attraverso il quale l'Amministratore di rete può gestire diversi aspetti della rete locale tra i quali il più importante è la definizione delle politiche di accesso alle risorse del sistema (es. file, cartelle, stampanti ecc.);
"Active Directory", elenco delle risorse presenti in una rete locale che consente, attraverso opportuni strumenti di amministrazione, di gestire le stesse in modo centralizzato;

“utente, user”, soggetto che mediante l’utilizzazione di credenziali d’accesso valide può accedere ai servizi di un sistema informatico conformemente ad un profilo per esso definito dall’Amministratore;

“username”, nome identificativo di un utente che, unitamente ad una password, consente l’accesso ad un sistema informatico protetto;

“password”, parola chiave che, unitamente ad uno username, consente l’accesso ad un sistema informatico protetto; normalmente viene definita**:**
forte se non è riconducibile all’utente che l’ha generata (nome, cognome, data di nascita, nome della figlia ecc.) e se in caso di attacco di forza bruta è in grado di resistere alla decodifica per un tempo ragionevolmente lungo se paragonato all’attuale sviluppo tecnologico in ambito informatico.
debole se non presenta alcuna delle caratteristiche sopra citate e non consente per questo un accettabile livello di sicurezza.

“policy”, politiche di accesso alle risorse di un sistema gestite generalmente a livello centralizzato;

“gruppo di protezione”, insieme di utenti utilizzato per gestire gli accessi alle risorse di un sistema informatico centralizzato;

“file sharing”, servizio di condivisione file, consiste nella facoltà di un computer di mettere a disposizione di altri utenti del sistema informatico i file in esso contenuti secondo predeterminate policy**;**

“virus informatici”, programma in grado di produrre effetti più o meno dannosi a carico di uno o più sistemi informatici interconnessi contro la volontà dei gestori del sistema stesso**;**

“TCP/IP”, insieme di protocolli che consentono a computer con sistemi operativi anche diversi di dialogare tra loro**;**

“sniffing”, attività svolta a mezzo di particolari strumenti software e/o hardware che consente di “leggere” i dati in transito in una rete di computer ed eventualmente carpirne informazioni normalmente non accessibili (credenziali d’accesso a sistemi remoti, e-mail, flussi di connessioni ad internet ecc.);

“antivirus”, software in grado di individuare, bloccare o eliminare virus informatici o codice maligno ed eventualmente riparare i danni dagli stessi provocati;

“definizioni (o firme) dei virus”, insieme di informazioni che consentono al software antivirus di riconoscere i virus informatici o eventualmente del codice maligno;

“backup”, procedura di salvataggio di dati, può essere eseguita sia su supporti removibili che su computer diversi da quello di origine**;**

“restore”, procedura di recupero di dati salvati precedentemente attraverso una procedura di backup**;**

“file di log”, file di testo contenente informazioni relative ad un determinato processo normalmente generato dal processo stesso o dal sistema operativo**;**

“postazione di lavoro”, insieme di strumenti informatici e non normalmente utilizzati da un soggetto per lo svolgimento delle funzioni allo stesso assegnate all’interno della struttura dell’Ente**;**

LF-4. **NORMATIVA DI RIFERIMENTO**

Le norme e standard di riferimento:

- **Regolamento UE n. 2016/679** del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- **D. Lgs del 10 agosto 2018 n.** 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo
- **Direttiva UE n. 2016/680** del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
- **D.Lgs. 30 giugno 2003, n, 196**, recante: “Codice in materia di protezione dei dati personali“ e successive modificazioni;

ISO/IES 27001 Information Technology Security Techniques – Code of Practice for information security controls

ISPD-10003 Maggio 2018 Schema per la valutazione della conformità al regolamento europeo

Legge 22 aprile 1941, n. 633 e successive modificazioni, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (G.U. n.166 del 16 luglio 1941) e successive modifiche introdotte dalla L. 18-8-2000 n. 248, “Nuove norme di tutela del diritto di autore.” Pubblicata nella Gazzetta Ufficiale 4 settembre 2000, n. 206.

- notifica al Garante nei casi previsti;
- adozione delle misure tecniche e organizzative adeguate a garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato (privacy by design) e per garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente;
- vincolo al dovere di riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento;
- designazione del responsabile del trattamento a cui affidare mansioni importanti e di elevata professionalità, in fase di gestione dei dati personali;
- redazione del registro di trattamenti;
- formazione del personale;
- documentazione delle violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

LF-5. **ORGANIGRAMMA PRIVACY COMPITI E RESPONSABILITÀ**

Le figure identificate dalle disposizioni vigenti in materia di trattamento dei dati sono:

Titolare:
ha potere decisionale in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Il Titolare o su Sua delega il Direttore Generale nomina con contratto o atto giuridicamente valido, il responsabile del trattamento, insieme al quale pone in atto le misure tecniche ed organizzative congrue per garantire un livello di sicurezza adeguato al rischio.
Il titolare è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale. In particolare gli obblighi sono:

Direttore Generale:
Garantisce la qualità dei dati, le corrette modalità di raccolta, conservazione e trattamento degli stessi, anche da parte del personale della propria struttura, secondo quanto disposto dalla normativa in tema di trattamento dei dati, dai Provvedimenti del Garante e dal presente documento e vigila sul rispetto delle istruzioni impartite
Ha il compito di attuare le politiche di sicurezza nell'ambito del settore di competenza.
Ha il compito di suggerire e promuovere azioni che migliorino la sicurezza dei dati trattati dall'ente.
Deve segnalare al DPO l'avvio di nuovi servizi che prevedono il trattamento dei dati
Deve verificare che eventuali fornitori a cui sono affidati il trattamento di banche dati dell'Azienda Speciale abbiano competenze e modelli di gestione conformi alle indicazioni del nuovo regolamento europeo.

Il DPO (Data Protection Officer)
Ha il compito di:

- rendere noti al Titolare o al Responsabili di Settore/Area gli obblighi derivanti dal Regolamento europeo e conservare la documentazione relativa a tale attività di comunicazione o di consulenza;
- vigilare sulla corretta applicazione delle policy in materia di privacy,
- vagliare la corretta attuazione delle disposizioni contenute nel regolamento europeo, occupandosi, in particolare di verificare che i sistemi, sin dalla fase della loro progettazione rispettino la privacy (privacy by design) verificare la protezione di default di dati e sistemi (privacy by default), rilevare che venga garantita la sicurezza nei trattamenti dei dati;
- fornire agli interessati un riscontro circa i diritti previsti dal regolamento;
- garantire la conservazione dei documenti relativi ai trattamenti;
- verificare il tracciamento delle violazioni dei dati personali e la loro comunicazione agli interessati;
- verificare che titolare o responsabile effettuino la valutazione dell'impatto delle attività sulla privacy e controllare che venga richiesta l'autorizzazione all'autorità quando occorre;
- fungere da intermediario tra Titolare o Responsabile e autorità Garante in materia di trattamento dei dati;
- controllare che siano rispettati eventuali provvedimenti o richieste espresse dall' autorità Garante in materia di trattamento dei dati.
- elaborazione delle procedure inerenti il trattamento dei dati per le varie attività dell'ente;
- formare il personale in materia di privacy e trattamento dei dati;

5.1 l'Organigramma Inerente il Trattamento dei Dati

Nell' "organizzazione - privacy" dell'ente le figure coinvolte sono:
1. il "Titolare del trattamento": è la "figura" di vertice cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza dei dati.

2.. il "Direttore Generale": è un soggetto designato dal Titolare che, per esperienza, capacità ed affidabilità, fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza. Lo si definisce anche Responsabile "interno" per distinguerlo dal Responsabile "esterno" identificato dall'art 28 del GDPR. Relativamente ai trattamenti di dati personali trasversali a più strutture, per l'individuazione si applica il criterio del maggiore ambito decisionale attribuito o vi possono essere situazioni di co-responsabilità.

3. il "Responsabile trattamento" ai sensi dell'art 28 del GDPR: è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo, esterno all'Amministrazione, che, previa designazione formale del Direttore Generale, assume (su delega di quest'ultimo) poteri decisionali su un determinato trattamento e deve attenersi, nelle operazioni svolte, alle istruzioni ricevute.

4. l'Amministratore di Sistema: è, in ambito informatico, la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software utilizzati nei vari uffici, le reti locali e gli apparati di sicurezza, nella misura in cui tali attività di gestione e manutenzione consentano di intervenire sui dati personali.

5. l'incaricato del trattamento" (persona autorizzata al trattamento): è la persona fisica che, operando sotto l'autorità del Responsabile, effettua le operazioni di trattamento dei dati, attenendosi alle istruzioni ricevute.

6. il DPO Data Protection Officer: è il soggetto che, coadiuva il Titolare ed il Responsabile di Area e gli incaricati nella corretta gestione ed applicazione dei principi definiti dal Regolamento Europeo in termini di data Protection.

7. l'Interessato: è la persona fisica cui si riferiscono i dati personali (sono escluse dal campo di applicazione della normativa privacy le persone giuridiche).

Il Direttore Generale può nominare, per iscritto, quali Incaricati del trattamento, altresì, anche eventuali collaboratori "esterni" dell'Amministrazione (purché persone fisiche), a prescindere dal rapporto contrattuale intrattenuto con la stessa (ad es. stagisti, tirocinanti, ecc.), non dotati di potere decisionale autonomo, se stabilmente presenti negli uffici dell'Amministrazione.

Sanzioni:
il presente documento pone quindi una serie di istruzioni, direttive e linee guida poste a salvaguardia dei dati dei soggetti di cui l'Azienda Speciale gestisce i dati. Pertanto, l'eventuale inosservanza o violazione di tali istruzioni, direttive e linee guida costituisce infrazione disciplinare, nonché grave inadempimento ai sensi e per gli effetti dell'art. 1453 del Codice Civile, suscettibile di produrre le conseguenze previste dalla legge, nonché dal contratto collettivo nazionale e individuale di lavoro.

Nell'ambito dell'Ente vengono identificate le seguenti figure:

Area/Servizio	Posizione Organizzativa Prevista	Ruolo Trattamento dei Dati
Presidente	Rappresentante Legale	Titolare del trattamento dei dati è L'Azienda Speciale che è rappresentato legalmente dal Presidente
Direttore Generale	Direttore Generale	Direttore dell'Azienda, delegato dal Titolare per la nomina del trattamento dei dati sulla base del registro dei trattamenti stesso
Ufficio Risorse Umane e Organizzazione	Responsabile Ufficio	Designato del Trattamento dei Dati per l'area di competenza
Ufficio Legale	Responsabile Ufficio	Designato del Trattamento dei Dati per l'area di competenza
Ufficio Adempimenti Amministrazione Trasparente	Responsabile Ufficio	Designato del Trattamento dei Dati per l'area di competenza
Servizio Amministrativo e Finanziario	Responsabile di Servizio	Designato del Trattamento dei Dati per l'area di competenza
Servizio Tecnico – Autorizzazione agli scarichi in fognatura	Responsabile di Servizio	Responsabile Trattamento dei Dati per l'area di competenza
Servizio Tecnico - Pianificazione e Controllo	Responsabile di Servizio	Responsabile Trattamento dei Dati per l'area di competenza
Servizio Procedimenti Amministrativi e Sanzionatori	Responsabile di Servizio	Responsabile Trattamento dei Dati per l'area di competenza

LF-6. **COMPOSIZIONE DEL DOCUMENTO**

Il presente documento identifica le risorse da proteggere; che, in diverso modo, operano o comunque svolgono un ruolo significativo nei processi di trattamento dei dati.
A tal proposito, una volta individuati i dati da proteggere e gli asset utilizzati nella gestione degli stessi, tramite l'**Analisi dei Rischi**, sono state valutate e studiate le minacce e le vulnerabilità a cui tali risorse (i dati per l'appunto) sono sottoposte, in modo da potere valutare gli elementi che possono insidiare la protezione, l'integrità e la conservazione di ogni singolo dato personale trattato.

Dall'analisi dei rischi si è redatto un Piano di Sicurezza, tramite il quale si è provveduto a definire l'insieme delle misure fisiche, logiche ed organizzative adottate per tutelare le strutture e le risorse preposte al trattamento dati e quindi ai dati stessi.
Inoltre è stato definito un Piano di Verifiche delle misure adottate tramite il quale si provvederà ad accertare periodicamente la bontà delle misure individuate e ad apportare gli accorgimenti che si riveleranno necessari.
Per completezza, si è ritenuto utile e opportuno allegare al Piano della Sicurezza Informatica una serie di documenti che rendono, con immediatezza, intelligibile a quanti sono coinvolti, a vario titolo, nella politica di protezione e sicurezza dei dati personali adottata dal Titolare, nonché agli organi ispettivi, la politica di protezione e sicurezza dei dati personali (security and data protection policy).

LF-7. **REVISIONE DEI DOCUMENTI**

L'emissione e la revisione della Piano di Sicurezza del Sistema Informativo, avviene nel rispetto di regole precise e sotto la sorveglianza del Responsabile Area servizi alla Persona che garantisce uno sviluppo equilibrato e congruente con l'evoluzione del sistema informativo dell'Azienda.

Le regole da seguire per i vari tipi di documenti sono le seguenti:
Il PSSI contiene le politiche di sicurezza dell'Azienda. Eventuali modifiche della policy e revisioni del documento possono essere suggerite per iscritto da qualsiasi collaboratore dell'Azienda al Responsabile dell'Ufficio Risorse Umane e Organizzazione che le valuta e decide per un'eventuale modifica.

L'analisi dei rischi identifica i possibili eventi indesiderati che possono causare un danno alle risorse del sistema informativo. Una revisione del documento può essere determinata da una serie di motivi, variazione dell'impianto informativo, mutate condizioni organizzative o logistiche.

Le modifiche accolte dal Responsabile Area servizi alla Persona portano alla revisione del GDPR o della Analisi dei rischi. Va ribadito che l'iter di controllo e approvazione dei documenti, di cui ai punti precedenti, deve rispecchiare quello della prima emissione, a meno di cambiamenti del personale dell'ente o di cambiamenti organizzativi. Per ogni modifica effettuata si aggiorna progressivamente il numero della revisione.
La focalizzazione delle modifiche introdotte con le varie revisioni viene effettuata mediante un segno di evidenziazione del testo. Nel caso di revisione generale, i contenuti della procedura variati sono tali da considerarne una nuova impostazione.
L'aggiornamento dell'archivio cartaceo e di quello elettronico, relativi al PSSI, è compito del Responsabile Area servizi alla Persona.

Quando un Documento della sicurezza è revisionato, il Responsabile Area servizi alla Persona, conserva la copia superata in formato elettronico in un'apposita directory denominata "Doc_Sicurezza_Superati".
La copia in vigore del Piano di sicurezza, delle Procedure e delle Linee Guida sull'uso delle risorse del sistema informativo sono rese disponibili ai dipendenti dell'Azienda nella intranet aziendale.

Documento	Redazione	Approvazione	Distribuzione	Archiviazione
PSSI	Direttore Generale/Ufficio Risorse Umane e Organizzazione	Titolare	Ufficio Risorse Umane e Organizzazione	Ufficio Risorse Umane e Organizzazione
Procedure	Direttore Generale/Ufficio Risorse Umane e Organizzazione	Titolare	Ufficio Risorse Umane e Organizzazione	Ufficio Risorse Umane e Organizzazione
Linee Guida sull'Utilizzo delle Risorse Sistema Informativo	Direttore Generale/Ufficio Risorse Umane e Organizzazione	Titolare/Consiglio di Amministrazione	Ufficio Risorse Umane e Organizzazione	Ufficio Risorse Umane e Organizzazione

LF-8. **IDENTIFICAZIONE DELLE RISORSE E DELLE INFRASTRUTTURE**

Le risorse che in qualche modo intervengono nel trattamento dei dati del titolare sono identificate da:

- Luoghi fisici
- Banche dati
- Apparecchiature
- Personale

Di seguito verrà data una descrizione di questi elementi.

8.1 Luoghi Fisici

i luoghi fisici dove si svolge il trattamento dei dati sono identificati nel paragrafo capitolo 2

8.2 Sistema Informativo

8.2.1 Server e risorse elaborative

Il sistema informativo dell'ATO si compone di due server installati all'interno di locali con accesso selezionato. Sui server sono installati gli applicativi di gestione dei vari uffici e vengono salvati i file di produttività individuale; L'accesso alle banche dati avviene tramite Rete Locale.

Nella tabella Allegato1 al presente piano sono identificati i server, il sistema operativo installato e i servizi applicativi e le banche dati presenti sul server.

8.2.2 Networking

La rete LAN è una rete basata su sistema operativo Microsoft.
L'infrastruttura di rete dell'Azienda è costituita da una sala server, ubicata nell'edificio principale dell'Azienda, in cui sono installati i server del SIA.
Di seguito viene descritta l'infrastruttura di rete dell'Azienda

Infrastruttura di rete
Connessione alla rete Internet
Collegamento alla rete internet tramite linea in fibra
Gestione rete
Rete principale a cui accedono le postazioni di lavoro degli utenti Sottorete nella quale è installato il server di backup dei dati Gestione rete tramite dominio Microsoft In azienda è disponibile una rete WIFI riservata ai dipendenti ed accessibile tramite autenticazione di dominio È disponibile una connessione wifi pubblica su rete diversa dalla rete aziendale a cui possono accedere gli ospiti.
Apparati di protezione Perimetrale
La rete dell'Azienda è protetta da un firewall
Sala CED
Nel locale tecnico sono installati gli apparati di rete ed i server alimentati con batterie di continuità.
Accesso da remoto
Accesso da remoto da parte degli utenti tramite VPN e credenziali di autenticazione
Gestione Backup e Disaster Recovery
L'Azienda fa le copie di sicurezza dei dati • Backup in-site delle VM • Backup In-site del server DB Oracle • Backup criptato in cloud delle VM

8.2.3 Personal Computer

I PC in dotazione ai collaboratori dell'Azienda Speciale sono dotati di sistemi operativi Windows. Su ogni di essi è installato l'antivirus che viene periodicamente aggiornato.
L'accesso alle risorse di rete avviene tramite account composto da un identificativo e da una password.
L'aggiornamento del sistema operativo avviene automaticamente
Su ogni postazione di lavoro è installato un antivirus, che si aggiorna automaticamente
I computer accedono ad uno storage condiviso con cartelle profilate in relazione alla struttura organizzativa dell'ente. Su queste cartelle vengono salvati i file di produttività individuale (office).

8.2.4 Risorse Software

Gli applicativi software utilizzati dagli uffici sono descritti nell'Allegato 1

8.3 Registro dei Trattamenti

Il registro dei trattamenti descrive le banche dati gestite dal titolare e dai responsabili, ed è riportato nell'Allegato 2
Oltre alle banche dati sono anche identificati i soggetti a cui i dati vengono comunicati, siano essi enti Pubblici o aziende che per conto dell'Azienda Speciale svolgono un servizio.
Il registro viene aggiornato dal Responsabile di Area quando viene attivato un nuovo processo che prevede la gestione di banche dati.

- Calamità naturali
- Accesso non autorizzato
- Diffusione di software maligno
- Errori nel codice del sw
- Errori nella trasmissione dei dati
- Furti
- Errori umani
- Guasti alle apparecchiature

LF-9. **ANALISI DEI RISCHI**

I rischi a cui un sistema è sottoposto possono derivare dall'interno o dall'esterno, essere accidentali o volontari. Questi possono causare la perdita delle informazioni, la loro alterazione, o la non disponibilità.

Tra i possibili fattori di rischio del sistema rientrano:

Una volta identificati i possibili fattori di rischio associato alle diverse parti del Sistema Informatico (asset) è stata descritta la vulnerabilità ed il rischio ad essa associata.
Questo passaggio ha lo scopo di inquadrare i danni che potrebbero essere arrecati alle risorse del sistema e al soggetto di cui vengono trattati i dati.
L'analisi dei rischi è fondamentale per la identificazione le strategie da attuare per prevenire o ridurre il danno.
Un aspetto nell'analisi dei rischi consiste nello stimare le probabilità di accadimento degli eventi indesiderati (dimensione probabilistica).
Questa valutazione è stata fatta dal team di progetto in funzione dell'esperienza delle persone che hanno condotto l'analisi e in relazione alle conoscenze dell'ambiente e del sistema informativo dell'Azienda Speciale e tenendo conto delle contromisure adottate dall'ente per mitigare il rischio.

L'ultimo step per la quantificazione del rischio, consiste nel valutare la gravità che questi eventi accidentali possono causare, attuare degli interventi per migliorare la sicurezza del sistema che sono stati riportati nella tabella seguente.
Nel contesto del progetto, la stima degli inconvenienti causata dal verificarsi di certi eventi, non è stata fatta usando un criterio economico. Questo perché molti dei danni che si possono riscontrare sono difficili da quantificare, in quanto legati a disservizi causati ai cittadini, danni alle libertà e dignità degli interessati o alla perdita di immagine dell'Azienda. Anche in questo caso si è preferito identificare le priorità degli interventi da attuare in base all'esperienza del team di progetto e in funzione delle scelte economico/strategiche dell'ente.

9.1 RISULTATI DELL'ANALISI

Nell'Allegato 3 sono stati evidenziati i risultati dell'analisi condotta presso la sede principale dell'Azienda Speciale.

- Il Titolare delega il Direttore Generale quale designato alla nomina dei Responsabili al trattamento dei dati;
- I Direttore Generale qualifica responsabili esterni soggetti che per conto dell'Azienda svolgono servizi che prevedono il trattamento dei dati), che sono nominati dal Direttore Generale stesso quali responsabili esterni - fornitori (Le strutture all'interno dell'organizzazione complessiva dell'Azienda Speciale che si occupano del trattamento di dati personali, anche in relazione ai compiti loro assegnati, sono state individuate in base alla tipologia, all'entità, alla distribuzione e alla organizzazione delle attività svolte all'interno dell'ente.

LF-10. PIANO DI SICUREZZA

10.1 Misure organizzative

10.1.1 Nomina del personale incaricato al trattamento dei dati

Nell'ambito dell'ATO sono adottati una serie di procedimenti organizzativi volti a migliorare la sicurezza del sistema informativo.
Innanzitutto sono state identificati i ruoli e le responsabilità delle figure professionali che nell'ambito dell'ente trattano dati.
Le figure professionali identificate sono state formalmente incaricate attraverso una delega scritta che identifica competenze e responsabilità relative alla gestione del sistema informativo e al trattamento dei dati.

Le regole di nomina prevedono:
A tale scopo ciascun dipendente e collaboratore è incaricato ed autorizzato al trattamento dei diversi tipi di dati; gli incarichi - così come la responsabilità per la conservazione dei dati vengono conferiti personalmente al momento dell'inserimento di una nuova figura all'interno della struttura dell'azienda;
Ciascun incaricato può operare, per il trattamento dei dati, esclusivamente all'interno delle mansioni assegnate e in riferimento alle informazioni ed alle banche dati disponibili relative alla propria mansione;

Lavoratori a tempo determinato/stagisti: i soggetti che trattano dati dell'Azienda che, per qualifica attribuita od in relazione alla concreta attività svolta, non rivestono la figura di incaricati, sono stati opportunamente autorizzati al trattamento mediante specifica Nomina (stagisti, volontari ecc.).

10.1.2 Società e ditte addette alla Manutenzione degli strumenti di Elaborazione, dei software e delle reti informatiche

Nel caso in cui l'ente richieda l'intervento di ditte specializzate per interventi di assistenza e manutenzione, questi soggetti operano in base a specifica autorizzazione, recante nel dettaglio i compiti da svolgere. In particolare queste Ditte si trovano nella situazione di dover periodicamente svolgere lavori di manutenzione o, semplicemente, di verifica del funzionamento di un programma o di un dispositivo informatico. A tal fine è praticamente necessario accedere alle banche dati presenti sui personal computer o gestiti da programmi software, che si configura come un trattamento di dati personali che di per sé non è collegata allo scopo per cui i tecnici dell'azienda effettuano la propria attività.
Se l'attuazione delle misure di sicurezza, attraverso l'installazione di tool applicativi o apparati hw, viene affidata a soggetti esterni, il Titolare del trattamento riceve dall'installatore una descrizione scritta dell'intervento effettuato e delle operazioni realizzate.

- Cittadini
- Dipendenti dell'azienda
- Professionisti - Fornitori ed enti

10.2 Audit sulla corretta attuazione dei principi e delle regole di trattamento dei dati

Periodicamente, per verificare la corretta attuazione dei principi e delle misure organizzative e tecniche inerenti il trattamento dei dati e per rivedere l'analisi dei rischi ed il piano delle azioni da implementare per un miglioramento dei processi di gestione delle informazioni, verranno fatti degli audit.
Questa valutazione della compliance al REU 679/2016 verrà condotta dal DPO in collaborazione con i Responsabili di area e con l'amministratore di sistema. Al termine di questa attività viene prodotta una relazione nella quale vengono evidenziati anomalie riscontrate, piani ed attività di miglioramento che L'Azienda Speciale deve adottare.

10.3 Gestione profili utenti del sistema informativo

Nel caso di nuova assunzione o nel caso di variazione dell'organico sono adottate delle procedure di gestione degli utenti del sistema informativo. La policy prevede la comunicazione, da parte del responsabile dell'area presso la quale il dipendente presta/presterà servizio all'amministratore di sistema, delle variazioni delle mansioni e dei nuovi profili di accesso alle risorse del sistema informativo aziendale.
L'amministratore di sistema incaricato dovrà modificare i diritti di accesso alle risorse del sistema informativo e ai dati trattati attraverso strumenti informatici.

10.4 Gestione e comunicazione dell'Informativa

Come previsto dal RE 679/2016 L'Azienda Speciale ha predisposto dei modelli di informativa rivolti alle diverse categorie di soggetti interessati:
L'informativa è stata esposta, presso i vari uffici.
Una comunicazione (informativa sul trattamento dei dati) relativa alle regole e alle modalità di trattamento dei dati è stata pubblicata sul sito web dell'Azienda Speciale alla sessione Privacy.
La procedura PO-PSI-04 definisce le regole e le modalità di gestione dell'Informativa e delle modalità con cui acquisire eventualmente il consenso al trattamento dei dati.

10.5 Gestione della Trasparenze e della Pubblicità legale

La legge n. 69 del 18 giugno 2009, perseguendo l'obiettivo di modernizzare l'azione amministrativa mediante il ricorso agli strumenti informatici riconosce l'effetto di pubblicità legale agli atti e ai provvedimenti amministrativi pubblicati dagli Enti Pubblici sui propri siti informatici.

10.5.1 Pubblicazione on line e rispetto della privacy

Le regole sulla privacy dettate nel Decreto Legislativo n.196 del 2003 e del Reg. UE 679/2016, che garantiscono il diritto alla tutela dei dati personali, sono valide e debbono essere rispettate anche per i siti web (per es. dagli atti pubblicati vanno omessi i dati sensibili ossia quei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale).
L'albo pretorio contiene diversi provvedimenti che devono essere pubblicati per legge e che possono, a volte, fare menzione di alcuni dati sensibili strettamente indispensabili. Nel predisporre i documenti da

- la sala riunioni

affiggere, però, fermo restando il rispetto degli obblighi di legge sulla trasparenza delle deliberazioni adottate, occorre comunque rispettare la riservatezza degli interessati. La pubblicazione indiscriminata di informazioni personali può porsi, infatti, in contrasto con la legge sulla privacy quando ciò non sia necessario al raggiungimento delle finalità per le quali i dati sono stati raccolti.

Con la delibera n.17 del 19 aprile 2007 Allegato1 - Internet: sui siti di comuni e province trasparenza, ma con dati personali indispensabili – Il provvedimento costituisce una Linea guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali - il garante della privacy consente la diffusione di dati personali per finalità di trasparenza e di comunicazione nelle pubbliche Amministrazioni ma sempre nel rispetto dei principi di pertinenza, non eccedenza e indispensabilità dei dati da pubblicare su internet e pone nuovamente cautele e limiti di fronte alla pubblicazione di dati sensibili che inoltre, richiedono l'adozione di misure di sicurezza per garantire il trattamento dei dati con strumenti elettronici.

10.6 Sicurezza Fisica

La politica della sicurezza identifica i comportamenti che regolano l'accesso fisico a luoghi in cui sono conservati o custoditi dati personali o sensibili. A tale proposito si può identificare una classificazione degli stessi in:
Aree ad accesso non controllato
Aree ad accesso controllato
Aree ad accesso ristretto
Per ognuna di queste sono state definite delle modalità di gestione degli accessi e delle regole per quanto riguarda l'installazione delle apparecchiature.

10.6.1 Controllo degli accessi agli edifici

Le sedi dell'Azienda Speciale in cui viene effettuato il trattamento dei dati sono identificate nel capitolo 2 del presente PSSI. Nella tabella sottostante vengono identificati i sistemi di controllo degli accessi ai vari edifici e gli impianti di sicurezza installati

Sede	
Allarme antintrusione	Impianto allarme volumetrico che si attiva a orari predefiniti
Antincendio	Estintori e rilevazioni di fumi
Accesso principale dell'edificio	Porta di accesso costituita da portone in legno con chiave di sicurezza
Accesso all'edificio	Accesso secondario costituita da portone in legno con chiave di sicurezza
Distribuzione chiavi registrata	Chiavi di accesso all'edificio distribuite ad alcuni dipendenti dell'Azienda Speciale ed amministratori

10.6.2 Aree ad accesso non controllato

Sono quelle aree in cui il pubblico può accedere senza alcuna identificazione o misura di sicurezza. Rientrano in questa categoria:

- la Sala Server ›rse del Sistema Informatico attraverso password conosciuta unicamente
- l'Archivio documentale ›ono sono disposti esclusivamente in sala server.
- gli archivi contenenti banche dati su supporto cartaceo sono chiusi a chiave, nel caso siano ubicati nelle aree di permanenza del pubblico.

Regole relative a questi spazi

In queste aree non devono essere installate apparecchiature informatiche contenenti banche dati; non devono essere presenti apparecchiature collegate alla rete dell'azienda, se le stesse non sono presidiate da un operatore;
non devono essere presenti archivi documentali non adeguatamente protetti.

10.6.3 Aree ad accesso controllato

Sono quelle aree in cui può accedere solamente il personale dipendente dell'ente, nel caso in cui acceda del personale esterno questo deve essere accompagnato da un collaboratore dell'azienda. In questa tipologia rientrano anche le aree accessibili liberamente al pubblico che durante l'orario di apertura devono essere presidiate dai collaboratori dell'azienda. Rientrano in questi spazi:

Regole relative a questi spazi

In queste aree sono installate apparecchiature informatiche collegate alla rete interna.
Le stazioni di lavoro rispettano una serie di misure minime di sicurezza:

10.6.4 Aree ad accesso ristretto

Sono quelle aree in cui sono installate apparecchiature critiche quali server, apparati di rete, nonché documenti e banche dati cartacee. L'accesso a tali aree è consentito solamente al personale autorizzato.
I locali sono chiusi a chiusi e le chiavi custodite dalle persone autorizzate.
L'accesso del personale esterno è regolamentato dal Responsabile dell'Ufficio Tecnico.
Le aree ad accesso ristretto sono essenzialmente:

Regole di accesso SALA SERVER

Di seguito sono sinteticamente riportati i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati alle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi. Le misure riguardano la sala server dell'Azienda Speciale accessibile attraverso una porta dotata di serratura la cui chiave è in dotazione al responsabile dell'Ufficio Tecnico.

Accesso da parte del personale esterno

Il personale non dipendente che deve accedere alla sala server per la manutenzione degli apparati, degli applicativi software o degli impianti, deve registrare l'attività svolta sul registro di controllo degli accessi o attraverso dei rapporti di lavoro, indicando le proprie generalità, data, ed intervento eseguito.
Quando delle persone entrano nella Sala server il loro operato è supervisionato da un dipendente dell'azienda.
Nella tabella sottostante sono identificate le misure di protezione della sala server.

Sala Server	Regole Sicurezza
Accesso alla sala server	Porta blindata a doppia serratura

Autorizzazione Acceso	Chiavi distribuite al personale autorizzato (Direttore Generale e referente IT)
Allarme accesso	Allarme dell'edificio + Allarme specifico locali ATO
Antincendio	Rilevazione incendio - estintore in prossimità a CO2
Impianto energia elettrica	Controllo messa a terra svolto periodicamente
Aria condizionata per raffreddamento delle apparecchiature	presente
Installazione sistemi UPS	Apparati alimentati da Batterie di continuità

Regole di Accesso all'Archivio documentale

L'archivio dell'Azienda Speciale si distingue in archivio corrente, ed archivio storico.

L'archivio di deposito, sede secondaria di ATO, contiene i documenti di uso non più immediato o destinati alla conservazione. Le modalità di accesso a tale archivio è determinata dal Manuale di Gestione dell'Azienda Speciale, all'allegato "Gestione archivi analogici".

L'archivio corrente è identificato nelle scaffalature e negli armadi degli uffici dell'azienda, per i quali verranno identificate delle regole di accesso opportune.

L'archivio storico contiene dati e documenti, ed è ubicato in un locale dell'Azienda Speciale a cui possono accedere solamente le persone autorizzate.

L'accesso all'archivio è consentito solo al personale autorizzato, richiedendo la chiave all'ufficio protocollo. E' stato inoltre predisposto un registro M-PSI-21 in cui si devono identificare i documenti prelevati.

Archivio Documentale	**Regole Sicurezza**
Accesso all'archivio	Accesso tramite porta dotata di serratura le cui chiavi sono state consegnate al Direttore
Allarme accesso	Allarme dell'edificio
Antincendio	Nell'edificio è presente un impianto di rilevazioni dei fumi
Vigilanza notturna	Servizio attivato

10.6.5 Facility dell'edificio

Di seguito vengono identificate le misure adottate per la gestione della sicurezza e per la prevenzione di eventi naturali dannosi.

Impianto elettrico

L'impianto rispetta la normativa vigente. Eventuali interventi vengono svolti da ditte specializzate.

Periodicamente l'ufficio manutenzione fa un controllo della messa a terra dell'edificio.

Numeri telefonici di emergenza

I numeri telefonici delle ditte che curano l'assistenza hardware e software sono riportati in un elenco appeso nel locale ove sono custoditi il server di rete.

REGOLE DI MISURE DI SICUREZZA

In questo paragrafo vengono identificate le politiche per la gestione logica della sicurezza delle informazioni che interessano quindi l'accesso alle basi di dati attraverso gli apparati del sistema informativo.

10.7 Identificazione utenti del sistema informativo

Ogni utente può accedere alla rete del sistema informativo attraverso un identificativo (user id) univoco e password. L'identificativo e la password sono personali.
L'assegnazione dei diritti di accesso alla rete informatica o alla base di dati viene fatta dall'Amministratore di sistema informativo previa richiesta fatta dal responsabile di Area.

10.7.1 Password

La password è assegnata a ciascun utente in forma riservata. Allo stesso è consentito di variarla. La gestione della password prevede una serie di misure sotto riportate atte a rendere efficace l'utilizzo della stessa:
lunghezza minima 8 caratteri, con regole di complessità;
non deve essere comunicata ai colleghi;
non deve essere annotata su supporti accessibili o leggibili;
non deve contenere termini facilmente riconducibili all'incaricato.

10.7.2 Autenticazione degli utenti

Il sistema informativo prevede due livelli di autenticazione:
autenticazione per accesso alle risorse del sistema. L'Azienda Speciale, utilizza i servizi di autenticazione del sistema operativo Windows che prevedono la definizione della lunghezza minima delle password a 8 caratteri e l'utilizzo di una complessità nella definizione del codice di autenticazione.
autenticazione software dell'Ente. Per quanto riguarda gli accessi agli applicativi di business, sono state fornite precise istruzioni ai collaboratori sulla necessità di variare la password secondo le regole sopra indicate.
Autenticazione applicativa servizi esterni per quelle soluzioni la cui gestione viene fatta da enti esterni, si deve prevedere la creazione di un registro degli utenti. Le regole di gestione degli utenti sono definite dal Titolare di queste banche dati.
Accesso servizi esterni governativi – SPID – per l'accesso a servizi governativi, effettuati per l'adempimento di specifiche normative (ad es: trasmissione bilanci) si procede con utenze specifiche e/o SPID. Tali utenze sono rilasciate solamente ai dipendenti che trattano i dati coinvolti nei procedimenti.

10.7.3 Gestione Utenze amministrative

Nell'ambito della gestione della rete dell'Azienda Speciale sono state identificati dei soggetti che si occupano della gestione del sistema informativo (amministratori di sistema)
A questi soggetti sono assegnate credenziali di amministratore che devono essere gestite secondo quanto definito nella circolare AGID n 2-2017.
Le policy di gestione sono le seguenti:

Policy gestione utenze Amministrative	
Identificativo	L'identificativo dell'utenza amministrativa deve fare riferimento ad una persona
Password	La password deve essere di 14 caratteri (rif. circolare AGID 2 /2017)
Complessità della Password	La gestione delle parole chiave deve prevedere delle regole di complessità -scadenza ogni tre mesi e non riutilizzo per 3 volte di seguito (rif circolare AGID 2 /2017)
Conservazione delle parole chiave	Le password sono memorizzate in un file criptato con algoritmo AES/Rijndael (256-bit key). La password master di apertura del file è custodita in busta sigillata in un luogo sicuro a disposizione del titolare e del Direttore Generale

10.7.3.1.1 Gestione delle utenze amministrative di soggetti esterni

La gestione del sistema informativo vede la presenza di soggetti esterni quali i fornitori delle applicazioni software usate dagli uffici, soggetti che intervengono nella gestione della rete ecc che per operare devono disporre di utenze amministrative.

La gestione di queste utenze è in carico all'amministratore di sistema dell'Azienda Speciale che ha il compito di adottare le seguenti policy:

Policy gestione utenze Amministrative di soggetti esterni	
Permessi	Ad ogni soggetto deve essere assegnata una utenza amministrativa univoca i cui permessi sono limitati all'attività che lo stesso deve svolgere
Identificativo	L'identificativo dell'utenza amministrativa deve fare riferimento ad una persona
Password	La password deve essere di 14 caratteri
Complessità della Password	La gestione delle parole chiave deve prevedere delle regole di complessità
Conservazione delle parole chiave	I soggetti a cui sono assegnate queste utenze amministrative sono registrati in un file a disposizione dell'amministratore interno. Questo consente di tenere traccia dei soggetti a cui sono assegnate e di verificarne l'utilizzo

10.7.4 Le regole di autenticazione alla rete dell'Azienda

La gestione dell'assegnazione dei diritti di accesso viene fatta dall'amministratore di Sistema. Nel caso un collaboratore dell'Azienda Speciale si dimetta i diritti di accesso devono essere revocati attraverso una comunicazione all'amministratore del sistema da parte dell'ufficio del personale dell'Azienda Speciale. Id e password utilizzate non possono essere associate ad un altro utente.

Variazione incarico

Nel caso in cui il collaboratore ricopra un incarico diverso deve essere fatta una comunicazione all'Amministratore di Sistema il quale provvede a modificare i permessi di accesso alle banche dati e alle risorse del sistema informativo.

La richiesta, deve essere fatta in forma scritta all'Amministratore di Sistema da parte del Responsabile dell'Ufficio che accoglie il dipendente.

Nel caso un'utente dell'Azienda Speciale si assenti per un determinato periodo di tempo, l'Amministratore di sistema è in grado di cancellare la password impostata dall'utente e di creare un nuovo id in modo da poter accedere alle risorse del PC.
In modo analogo l'amministratore del sistema è in grado di creare degli utenti temporanei per accedere agli applicativi di business.

10.7.5 Comunicazione di variazione delle password

Per quegli applicativi e strumenti elettronici il cui accesso è consentito esclusivamente tramite credenziali di autenticazione, la cui gestione e variazione non è riconducibile all'ufficio informatico, la stessa deve essere gestita in forma controllata.
In ogni settore viene identificato un responsabile delle password che gestisce attraverso un registro elettronico o documentale l'elenco dei servizi applicativi esterni all'azienda
Nel caso di assenza prolungata dell'incaricato del trattamento dei dati il Responsabile di Area o un collaboratore dell'azienda, previa autorizzazione del responsabile, possono utilizzare le credenziali di autenticazione avvertendo l'incaricato dell'intervento effettuato.

10.8 Gestione degli Archivi documentali

L'Azienda Speciale gestisce archivi documentali contenenti sia dati personali che giudiziari.
Per quanto riguarda la gestione degli archivi cartacei l'ente ha adottato le seguenti regole:
nel caso di documenti archiviati in armadi collocati in luoghi non presidiati dai dipendenti ed accessibili al pubblico, (corridoi, sala riunioni, sala giunta e del consiglio) questi devono essere chiusi a chiave in modo da garantire la privacy e l'integrità delle informazioni contenute.

I **dati Personali Particolari e Giudiziari** necessariamente vanno custoditi in armadi dotati di serratura chiudibile a chiave.
Se durante le ore di lavoro, l'operatore dell'Azienda Speciale deve accedere ai documenti cartacei contenenti dati relativi ai cittadini dell'Azienda Speciale o dati relativi alla gestione dell'ente, gli stessi devono essere gestiti con attenzione in modo da non pregiudicarne la privacy o la sottrazione indebita.
Al termine della consultazione gli stessi devono essere riposti con cura negli armadi da cui sono stati prelevati.
Nel caso alcuni documenti contenenti dati personali, sensibili o dati classificati come importanti non siano più utili questi devono essere distrutti in modo da non risultare leggibili.
La gestione dei documenti cartacei compete ai responsabili di settore/area ognuno per le proprie competenze.

10.8.1 Regole chiusura Uffici ed Armadi

Uffici

Al termine dell'orario di lavoro gli uffici devono essere chiusi; le chiavi sono in possesso ad almeno due persone dell'ufficio ed una depositata presso la portineria dello stabile del proprietario dell'immobile (Città Metropolitana di Milano)

Armadi (nel caso in cui gli uffici non siano chiudibili): al termine della giornata lavorativa i documenti contenenti dati sensibili vanno riposti negli armadi che devono essere chiusi. Le chiavi sono depositate in un armadio chiuso, la cui chiave viene custodita secondo le disposizioni del Responsabile dell'ufficio.

10.8.2 Gestione della comunicazione di dati tramite documenti Cartacei

In questo paragrafo vengono identificate le regole per la trasmissione dei documenti cartacei nell'ambito dell'Azienda Speciale.

Le regole adottate dall'azienda prevedono:
le comunicazioni in ingresso vengono protocollate dall'ufficio del protocollo, e i documenti classificati come riservati o contenenti dati sensibili vengono registrati a inoltrati all'ufficio competente come riservati;
Nel caso di comunicazioni verso l'esterno, la protocollazione della posta è gestita dai singoli uffici.
Per la trasmissione di documenti tra uffici dell'azienda, compresi lo smistamento della posta da parte del protocollo, deve rispettare una serie di principi in particolare quello di necessità e pertinenza. Cioè i dati possono circolare solo per ragioni di servizio e per la necessità dei singoli uffici; inoltre la corrispondenza non deve passare indiscriminatamente da più persone evitando passaggi superflui.

10.9 Sicurezza della rete informatica

10.9.1 Attacchi alla sicurezza Informatica

Senza la pretesa di offrire una classificazione formale e completa, possiamo considerare gli attacchi come violazioni delle proprietà di sicurezza precedentemente enunciate. I tipi di attacchi possono essere dunque:

- intercettazioni (violano la proprietà di segretezza dell'informazione);
- alterazioni (violano il requisito di integrità);
- generazioni (violano i requisiti di autenticità e di non-ripudio);
- interruzioni (minacciano la disponibilità del sistema).

Nella tabella sono elencate le caratteristiche principali di ogni categoria di attacco, insieme ad alcuni esempi presi da contesti reali.

10.9.2 Sicurezza della rete

La rete consente alle varie postazioni di lavoro di collegarsi alle unità centrali di elaborazione dei dati. Una rete locale mediante opportuni apparati si può poi collegare ad internet, è intuitivo che i livelli di protezione del sistema informativo cambiano se si verifica quest'ultima condizione.

La rete dell'Azienda Speciale è configurata mediate la definizione di un **Dominio di rete** a cui accedono gli utenti previa autenticazione. Per quanto riguarda la rete locale la politica di gestione degli indirizzamenti prevede l'utilizzo di uno schema di indirizzi IP che utilizzano il servizio DHCP.

Nela tabella di seguito riportata vengono descritte le misure di sicurezza informatica adottate dall'Azienda Speciale

Gestione Rete
Sicurezza perimetrale

Gestione Rete	
Connessione rete internet	Connessione alla rete di internet attraverso linea Fibra Gestione dell'accesso tramite Proxy pfsense su cui è stata configurata una openVPN aziendale
Apparati Protezione perimetrale	Firewall installato ha le seguenti funzionalità IPS Content filtering VPN (destinata solo agli amministratori)
Configurazione ed installazioni delle Postazioni di lavoro e Server	
Aggiornamento dei sistemi operativi	SERVER: Gli aggiornamenti delle macchine server vengono controllati settimanalmente ed installati quando presenti. PdL: sulle postazioni di lavoro è attivo il servizio di aggiornamento in automatico del sistema operativo e dei software di sicurezza
Viene tenuta traccia delle attività di eventuali interventi di manutenzione dei server di rete?	Gli interventi di installazione o manutenzione della rete informatica sono tracciati con dei rapportini di intervento che specificano le attività realizzate da parte di ditte esterne
Configurazione delle PdL	L'installazione delle postazioni di lavoro viene fatta installando un set predefinito di applicazioni software e tool di sicurezza
	Nel caso di cattivo funzionamento di una PDL viene fatta la reinstallazione
Gestione Apparati e dei Dispositivi di Rete	
Gestione apparati rete	L'azienda ha installato un tool per la gestione dell'inventario degli apparati di rete - OCS inventory
Gestione aggiornamenti	La gestione degli aggiornamenti è gestita tramite server WSus
Aggiornamento dei firmware degli apparati di sicurezza (firewall router ecc..).	Verifica periodica (6 mesi) degli aggiornamenti e loro installazione
tool di protezione delle PdL e dei Server	
L'antivirus	Antivirus professionale con console centralizzato Bit defender Gravity Zone Business Funzionalità principale • Anti-Virus Web • Anti-Virus Posta • Protezione dal phishing
Configurazioni antivirus	controllo dispositivi esterni quando viene collegato al PC pianificazione settimanale scansione completa del computer
Protezione PC	Sulle postazioni di lavoro è attivo un firewall personale
Strumenti di Protezione perimetrale: Antispam	Il servizio di posta è protetto da un servizio antispam del provider di posta elettronica
Presenza di sottoreti	Il server di backup è su un'altra subnet. E' solo il server di backup che accede alle 2 lame del server e non il viceversa

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- identificare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

LF-11. VIOLAZIONE O PERDITA DEI DATI

Nel caso in cui ci sia una violazione dei dati personali, intesa come la "violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ad informazioni personali trasmesse, memorizzate o comunque trattate, l'ente è tenuto a darne comunicazione all'autorità competente.
Entro 72 ore dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante (tramite apposito modello Allegato1 pubblicato sul sito www.garanteprivacy.it) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali.

La comunicazione deve:
Inoltre, quando la violazione dei dati personali è suscettibile di danno per i diritti e le libertà delle persone fisiche, il Titolare deve comunicare la violazione anche all'interessato, senza ingiustificato ritardo, descrivendola con un linguaggio semplice e chiaro (salve circostanze al verificarsi delle quali la comunicazione è esclusa). I dettagli sono descritti nella Procedura PO-PSI-05.

LF-12. FORMAZIONE

La gestione della sicurezza informatica in una qualsiasi organizzazione vede coinvolte in modo stretto gli utenti del sistema. Ciò richiede un piano di formazione rivolto ad ogni dipendente che utilizza le risorse informatiche dell'organizzazione. L'obbiettivo è quello di creare la "cultura della sicurezza" attraverso una serie di attività volte ad illustrare i provvedimenti ed i comportamenti da adottare per migliorare la sicurezza nel trattamento dei dati. Il piano è stato studiato, organizzato e suddiviso sulla base delle specifiche esigenze di ciascuna area in relazione alla natura dei dati trattati e dei rischi generici o specifici che incombono sui dati, nonché dei criteri e delle modalità di evitare tali rischi.

Periodicamente il Responsabile Area servizi alla Persona trasmette a tutti i dipendenti del materiale informativo in cui sono riportate le principali regole di gestione ed utilizzo delle risorse del sistema informativo.

12.1 Piano di formazione

Per le risorse umane, che hanno un ruolo chiave nel trattamento di dati personali, è stato fatto un corso di formazione inerente i principi fondamentali del REU 679/2016. I contenuti essenziali del piano di formazione sono:

- ragioni della nuova normativa
- ambito di applicazione materiale e territoriale
- principi generali
- diritti dell'interessato
- titolare e responsabili del trattamento
- data Protection Officer
- obbligo di tenuta di un "Registro delle attività di trattamento" ed effettuazione della "valutazione di impatto sulla protezione dei dati"
- obblighi di consultazione con l'autorità di controllo
- codici di condotta e certificazione
- trasferimento dei dati e problematiche di diritto extracomunitario
- principi legislativi e comunitari
- funzionamento della normativa nell'ambito dei diritti del cittadino
- crimini informatici, frodi, abusi, danni, casistica
- rischi possibili e probabili cui sono sottoposti i dati
- misure di sicurezza tecniche ed organizzative e comportamentali deputate alla prevenzione dei rischi
- comportamenti e modalità di lavoro per prevenire i rischi

Tale formazione viene erogata mediante supporti informativi cartacei, elettronici e/o telematici.

Il piano di formazione verrà erogato anche per i dipendenti neo assunti che nell'ambito delle loro mansioni svolgono un ruolo di responsabili del trattamento dei dati.

- Acquisizione di informazioni inerenti le politiche del fornitore in merito alla gestione dei dati
- Definizione di criteri di Selezione del fornitore
- Qualifica del fornitore ed Inserimento dello stesso nell'elenco dei fornitori accreditati
- Autorizzazione del fornitore al trattamento dei dati quale responsabile esterno
- Criteri di sorveglianza dell'operato del fornitore se la gestione dei dati costituisce un processo critico

LF-13. GESTIONE DEI FORNITORI A CUI SONO ASSEGNATI DEI SERVIZI CHE PREVEDONO IL TRATTAMENTO DI BANCHE DATI

L'Azienda Speciale nell'ambito della del proprio operato ha identificato dei soggetti esterni ai quali ha affidato la gestione di alcuni servizi che prevedono il trattamento di banche dati. Questo implica che queste organizzazioni trattano, assumendo decisioni autonome, queste informazioni di cui L'Azienda Speciale è Titolare.
Per ottemperare a quanto previsto dal regolamento europeo in materi di data protection l'ente ha definito una procedura di valutazione e gestione del fornitore PO-PSI-03 nella quale sono definiti i criteri per valutare la capacità dello stesso di gestire in modo corretto queste informazioni:
La procedura prevede alcune fasi che partono dalla definizione di criteri di qualifica, prevedono un processo autorizzativo da parte del titolare a trattare determinate informazioni, e la definizione congiunta con l'ente delle policy per il trattamento dei dati secondo un iter di seguito riassunto:

13.1 Qualifica dei Fornitori che trattano dati per conto dell'Azienda

Nel caso in cui l'ente assegni all'esterno dei servizi di competenza dell'Azienda Speciale che prevedono il trattamento di dati personali, prima di procedere all'assegnazione dell'incarico devono essere verificare le misure organizzative e tecnologiche attivate in tema di trattamento dei dati.
A tale scopo il responsabile del procedimento invia al fornitore una scheda per la raccolta dei dati sia di carattere generale che inerenti le modalità di gestione delle informazioni.
La scheda presente come allegato alla procedura PO-PSI-03 deve essere restituita al responsabile del procedimento con le informazioni richieste e sottoscritta da parte del rappresentante legale del fornitore.

13.2 Valutazione delle caratteristiche del fornitore

Il responsabile del procedimento unitamente al Responsabile Area servizi alla Persona e al DPO valuta, in funzione della tipologia del servizio che il fornitore deve erogare, se le policy di gestione dei dati sono adeguate al livello di criticità e rischio implicito nel trattamento.
Nel caso siano state riscontrate delle difformità rispetto alle politiche di sicurezza dell'ente viene fatta una comunicazione in cui si chiedono maggiori delucidazioni od un adeguamento agli standard di sicurezza previsti dall'Azienda e presenti nelle linee guida emanate da AGID.

LF-14. AUDIT DELLA SICUREZZA

14.1 Verifiche generali

Le verifiche sulla corretta applicazione delle misure di sicurezza per la protezione dei dati e delle informazioni gestite dall'Azienda Speciale nel suo complesso e delle misure particolari in riferimento esplicito a quelle previste dalla legge sul trattamento dei dati personali, sono affidate ai Responsabili del trattamento al DPO e al Responsabile Area servizi alla Persona che si avvale di apposite liste di controllo.
Le singole funzioni sono comunque tenute alle verifiche previste nella tabella di sintesi sotto riportata.

MISURE DA VERIFICARE	OGGETTO DELLE VERIFICHE	CADENZA	RESPONSABILE
Organizzazione			
Aggiornamento GDPR/PSSI	Controlli periodici, ed aggiornamento del PSSI	periodica	DPO
Outsourcing	Verifica criteri di sicurezza dei fornitori	a Campione	Direttore Generale/ DPO
Incarichi inerenti la sicurezza ed il trattamento dei dati	Controlli periodici degli incarichi, dei compiti e delle responsabilità.	periodica	Direttore Generale
Analisi dei rischi	Analisi dei rischi e delle contromisure da adottare per contrastarli.	periodica	Direttore Generale / DPO
Autorizzazioni all'accesso	Almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione	periodica	Amministratore di sistema
Autorizzazioni all'accesso	Rilasciate e revocate periodicamente	costantemente	Amministratore di Sistema
Piano di formazione	Attivazione del piano di formazione per nuovi collaboratori dell'Azienda Speciale	periodica	Direttore Generale / DPO
Protezione fisica			
Protezione delle aree e dei locali	Controlli periodici degli impianti e dei sistemi di sicurezza	periodica	Responsabile servizio manutenzione (Città Metropolitana di Milano)
Antincendio	Manutenzione periodica secondo le indicazioni dell'installatore	periodica	Responsabile servizio manutenzione(Città Metropolitana di Milano)
UPS	Manutenzione preventiva UPS Secondo le istruzioni del costruttore.	periodica	Amministratore di Sistema
Controllo accessi fisici ai locali	Controlli periodici dei sistemi che regolano l'accesso agli edifici, agli archivi o alle aree ad accesso	periodica	Responsabile servizio manutenzione (Città

	ristretto.		Metropolitana di Milano)
Protezione Logica			
Criteri e procedure per assicurare l'integrità dei dati	Controlli accessi banche dati. Controllo utilizzo modalità di autenticazione	periodica	Amministratore di Sistema
Codici identificativi personali	Disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore	Sempre	Amministratore di Sistema
Restrizioni di accesso per via telematica	Controllo account sistema informativo	periodica	Amministratore di Sistema
Sicurezza delle trasmissioni dei dati	Controlli periodici log dei firewall	mensile	Amministratore di Sistema
Sistema Informativo			
Misure di sicurezza della rete informatica	Verifica buon funzionamento Verifica aggiornamento	periodica	Amministratore di Sistema
Patching	Aggiornamento periodico dei sistemi informativi dei server Aggiornamento periodico dei sistemi informativi dei client	Ogni mese	Amministratore di Sistema
Back-up Dati	Verifica back-up dei dati e dei dati di sistema e efficienza apparecchiature e supporti.	Quotidiana	Amministratore di Sistema
Re impiego dei supporti di memorizzazione	Controlli sulla recuperabilità delle informazioni precedentemente contenute	costantemente	Amministratore di Sistema

LF-15. Elenco delle Procedure allegate al presente documento

Id Procedura	Descrizione	Responsabile archiviazione
PO-PSI-01	Gestione utenti del sistema informativo	Direzione Generale
PO-PSI-02	Gestione delle copie di sicurezza dei dati	Direzione Generale
PO-PSI-03	Gestione dei fornitori a cui sono stati affidati dei trattamenti	Direzione Generale
PO-PSI-04	Gestione dell'informativa e del consenso al trattamento dei dati	Direzione Generale
PO-PSI-05	Gestione Incidente Informatico - Data Breach	Direzione Generale
PO-PSI-06	Gestione valutazione di Impatto sulla protezione dei dati	Direzione Generale