ACQUEDOTTO POIANA S.P.A.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

redatto ai sensi del D.Lgs. 231 dell'8 giugno 2001 e ss.mm.ii.

PARTE SPECIALE

REATI INFORMATICI E DIRITTO D'AUTORE

AII.1 - UTILIZZO CONSAPEVOLE DEGLI STRUMENTI INFORMATICI

Versione	12
Dirigente delegato	Direttore Generale
Organo di approvazione	Consiglio di Amministrazione
Data di approvazione	28 gennaio 2026

Indice

1 PREMESSA 1
2 SOGGETTI CON RUOLI RILEVANTI E RAPPORTO FRA COLLABORATORI ED ENTE 2
3 BUSINESS COMPLIANCE 6
3.1 D. LGS. 231/01 – RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI. 6
3.2 REGOLAMENTO (UE) 2016/679 E D. LGS. 196/03 8
3.3 PORNOGRAFIA E PEDOPORNOGRAFIA 8
3.4 DIRITTO D'AUTORE 9
3.5 SOCIAL MEDIA 9
3.6 ATTIVITÀ IN PAESI ESTERI 10
4 ISTRUZIONI GENERALI PER L'UTILIZZO DEGLI STRUMENTI E DEI SERVIZI. 11
5 SICUREZZA DEI DATI E DEI SISTEMI. 12
5.1 COLLABORATORI ED UTILIZZO DEL SISTEMA INFORMATIVO E DEI DATI 13
5.2 CREDENZIALI DI AUTENTICAZIONE. 14
5.3 SUPPORTI MAGNETICI O CARTACEI: UTILIZZO, RIUTILIZZO E LORO DISMISSIONE. 15
5.4 PROTEZIONE ANTIVIRUS. 15
5.5 FIREWALL 16
5.6 SISTEMI DI MOBILE DEVICE MANAGEMENT (MDM) 16
5.7 POLITICHE DI BACKUP 17
5.8 PATCHING 17
6 POSTA ELETTRONICA E INTERNET. 17
6.1 INTERNET 18
6.2 POSTA ELETTRONICA ED INDIRIZZI MAIL AZIENDALI. 19
6.3 IL RAPPORTO FRA OUTSOURCER, FORNITORI E ACQUEDOTTO POIANA SPA 21
6.4 WIRELESS ACCESS POLICY 22
6.5 BYOD PRESSO ACQUEDOTTO POIANA SPA 22
6.6 SMART WORKING 23
6.7 ARCHIVI, DATI E DOCUMENTI. 24
7 CONTROLLI 26
8 VALIDITÀ E REVISIONE DELLA POLICY AZIENDALE. 28

1 Premessa

Le tecnologie informatiche stanno assumendo un ruolo sempre più importante all'interno delle organizzazioni: da un lato, è possibile raccogliere, a costi estremamente bassi, una grande quantità di dati che necessitano di essere analizzati, classificati e gestiti per potersi tradurre in informazioni; dall'altro, un utilizzo inconsapevole, distratto, se non addirittura, fraudolento può comportare pesanti conseguenze sia per i soggetti cui le informazioni si riferiscono che per gli enti che gestiscono i dati.
Di questi aspetti si è reso conto il Legislatore che, progressivamente, ha cercato di regolamentare finalità e le modalità di esecuzione del trattamento dati, tenendo conto di tutti i diversi aspetti che hanno a che fare con il Sistema Informativo. Questo si è tradotto in una serie di provvedimenti che impongono l'adozione di accorgimenti tecnici, procedurali ed organizzativi.

Questo documento si propone di rappresentare una sintesi di prescrizioni e accortezze, fornendo agli utenti dei sistemi informativi un unico insieme di indicazioni operative cui uniformare il proprio comportamento, nel rispetto di alcuni principi e valori etici che rappresentano le fondamenta dell'architettura organizzativa di Acquedotto Poiana SpA. Nella redazione si è tenuto conto di alcuni disposti di Legge, delle indicazioni fornite da enti ed istituzioni pubbliche nazionali ed internazionali (AgID[1], ENISA[2], …) e dei principali standard internazionali tra cui:

- Codice Civile;
- Codice Penale;
- L. 633 del 22/04/1941 – "*Protezione del diritto d'autore e di altri diritti connessi al suo esercizio*" (G.U. n.166 del 16/07/1941), s.m.i.;
- L. 300 del 20/05/1970 – "*Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento*" (G.U. 131 del 27/05/1970), s.m.i.;
- D.Lgs. 231/01 – "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300*" (G.U. 140 del 19/06/2001) s.m.i.;
- Regolamento (EU) 2016/679 - - "*Regolamento 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. 196/03 – "*Codice in materia di protezione dei dati personali*" (G.U. 174 del 29/07/2003) come modificato dal D.Lgs. 101 del 10 agosto 2018 nonché provvedimenti specifici in materia di privacy predisposti dall'Autorità Garante;
- D.Lgs. 82/05 – "*Codice dell'Amministrazione Digitale*" (G.U. 112 del 16/05/2005, S.O. 93) s.m.i.;
- Direttiva 2022/2555 "*Relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE)*

[1] L'Agenzia per l'Italia Digitale (AgID), istituita dal Governo Monti, è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione.
[2] L'Agenzia dell'Unione Europea per la Cybersicurezza ("ENISA", dal nome originale inglese European Network and Information Security Agency) è stata istituita nel 2004 e contribuisce alla politica dell'UE in materia di sicurezza nel settore informatico.

2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)" (G.U.U.E. 333 del 27/12/2022);

- Regolamento (UE, Euratom) 2023/2841 "*del 13 dicembre 2023 che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione*" (G.U.U.E. L del 18/12/2023).
- ENISA – "*Communication network dependencies for ICS/SCADA Systems*" – Dicembre 2016;
- AgID – CIRCOLARE 18 aprile 2017 , n. 2/2017 – "*Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»*";
- ENISA – "Handbook on Security of Personal data Processing" – Dicembre 2017;
- ENISA – "*Good practices on interdependencies between OES and DSPs*" – Novembre 2018;
- ENISA – "*Guideline on security measures under the EECC*" – July 2021;
- ENISA – "*Identifying emerging cyber security threats and challenges for 2030*" – Marzo 2023;
- ENISA – "*Good practices for supply chain cybersecurity*" - Giugno 2023
- ISO 27002:2022 – "*Information security, cybersecurity and privacy protection*"

Stante l'importanza che Acquedotto Poiana SpA riconosce alla presente Policy come atto regolamentare, **il mancato rispetto o la violazione delle regole in essa contenute sarà perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.**

2 Soggetti con ruoli rilevanti e Rapporto fra collaboratori ed ente

Nell'ambito della presente Policy, assume un ruolo rilevante la figura del **Direttore Generale**, cui il Consiglio di Amministrazione ha delegato le responsabilità in materia di Reati Informatici e Trattamento Dati. Nel prosieguo, ogni accezione al **Delegato** sarà a lui riferibile.
Un'altra figura rilevante è il **Referente Informatico**, soggetto dotato di competenze tecniche ma privo di poteri decisionali che rimangono in capo al Delegato.

Tutti i collaboratori hanno il dovere di utilizzare gli strumenti messi a loro disposizione per lo svolgimento delle mansioni loro assegnate nell'ambito del rispetto dei doveri di diligenza e fedeltà, imposti dal **Codice Civile**:

Art. 2104
Diligenza del Prestatore di Lavoro

1. Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale.
2. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende.

Art. 2105
Obbligo di Fedeltà

1. Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio.

Al fine di tutelare e proteggere la propria organizzazione, al Datore di Lavoro è concesso di effettuare controlli preventivi e continui sull'uso degli strumenti assegnati e, più in generale, sull'intero trattamento dati attuato dal collaboratore, essendo, da un lato, i dispositivi assegnati qualificabili come strumenti di lavoro la cui utilizzazione per fini personali è preclusa e, dall'altro, essendo i dati trattati un vero e proprio patrimonio aziendale.
Recita, infatti, il **Codice Penale**:

Art. 621
Rivelazione del contenuto di documenti segreti

Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto deriva nocumento, con la reclusione fino a tre anni o con la multa da euro 103 a euro 1.032.
Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi.
Il delitto è punibile a querela della persona offesa.

Art. 622
Rivelazione di Segreto Professionale

Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da euro 30 a euro 516.
La pena è aggravata se il fatto è commesso da amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci o liquidatori o se è commesso da chi svolge la revisione contabile della società.
Il delitto è punibile a querela della persona offesa.

Art. 623
Rivelazione di segreti scientifici o industriali

Chiunque, venuto a cognizione per ragione del suo stato o ufficio, o della sua professione o arte, di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche o applicazioni industriali, le rivela o le impiega a proprio o altrui profitto, è punito con la reclusione fino a due anni.
Il delitto è punibile a querela della persona offesa.

Premesso, quindi, che l'utilizzo del sistema informativo deve sempre ispirarsi al principio della diligenza e correttezza, Acquedotto Poiana SpA intende evitare che comportamenti, spesso inconsapevoli e non deliberati o fraudolenti, possano causare problemi, danni o minacce alla sicurezza o costituire vere e proprie violazioni di Legge. Oltre a ridurre il rischio di commissione dei reati, questa policy riduce il rischio di depauperazione del patrimonio di asset fisici od immateriali (relazioni, know how, dati, immagine, brand,…) ma anche la possibilità di Data Breach e di interruzione del flusso operativo.

Va precisato esplicitamente che **l'insieme dei controlli adottati non è in alcun modo preordinato al controllo a distanza dei lavoratori**, nel rispetto dell'art. 4 della L. 300/70, come modificato dall'articolo 23 del D.Lgs. 151/2015 - *Razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese* - attuativo del Jobs Act:

Art. 4
Impianti audiovisivi e altri strumenti di controllo

> *1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.*
> *2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*
> *3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.*

Per concretizzare questi principi, sono state, **esplicitamente evitate** situazioni in cui siano anche solo possibili:

- la registrazione mediante sistema di videosorveglianza degli accessi o della permanenza nei punti di ristoro;
- la lettura e la registrazione sistematica dei messaggi di posta elettronica;
- la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer portatili e dei dispositivi affidati in uso.

Acquedotto Poiana SpA riconosce come imprescindibili i valori di cui al **Codice Etico** che qui si richiama esplicitamente, improntando su di esso il proprio operato e imponendone il rispetto a tutti i collaboratori, business partner e, in generale, a tutti i destinatari del Modello di Organizzazione, Gestione e Controllo ("MOG") di cui l'Ente si è dotato.

Oltre al rispetto del Codice Etico, ciascun collaboratore, business partner e destinatario del MOG ha il dovere di segnalare, nel rispetto della **Policy di Whistleblowing** di cui l'Ente si è dotato e che costituisce un allegato al MOG, eventuali "violazioni", come definite dall'art. 2, c.1 lett. a) del D.Lgs. 24/2023, ovvero:

1) illeciti amministrativi, contabili, civili o penali;
2) condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231, o violazioni dei modelli di organizzazione e gestione;
3) illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
4) atti od omissioni che ledono gli interessi finanziari dell'Unione;
5) atti od omissioni riguardanti il mercato interno comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale;
6) atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nei numeri 3), 4) e 5).

3 Business compliance

Se si concorda con l'assunto che ogni Ente, pubblico o privato, si propone come fine ultimo la creazione di valore per sé e per la collettività, non è pensabile prescindere dal considerare il rischio come fonte di potenziale danno nel lungo periodo. Ecco che, quindi, l'obiettivo di minimizzazione del rischio deve essere un principio fondante per qualsiasi collaboratore di Acquedotto Poiana SpA.
Nell'ambito della gestione del rischio, il rispetto della normativa "rilevante" da parte di ogni collaboratore e partner rappresenta uno degli aspetti più critici, soprattutto in un Paese come il nostro. A tal fine, il rispetto delle norme deve essere previsto all'interno delle procedure aziendali ma solo la piena conoscenza delle principali norme di riferimento e dei principi che stanno alla base delle politiche aziendali di *compliance* da parte di tutti garantisce all'azienda di rispettare il contesto normativo di riferimento.

Per questo, nel prosieguo, verranno riportati i principali ambiti legislativi ed i principi che sottendono il rispetto dei disposti regolatori.

3.1 D. Lgs. 231/01 – Responsabilità amministrativa degli Enti.

Il D.Lgs. n. 231 - "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*" ha introdotto nell'ordinamento giuridico italiano un complesso ed innovativo sistema sanzionatorio che prefigura forme di responsabilità degli Enti per effetto di azioni commesse nel loro interesse o a loro vantaggio da apicali e loro subordinati in relazione ad alcune fattispecie di reato.
A tal fine, la presente policy intende stigmatizzare specifici comportamenti e suggerire accorgimenti volti a ridurre la possibilità che vengano compiuti reati rientranti nel novero dei reati presupposto di natura informatica o che vengano utilizzati asset informatici aziendali quale mezzo per poter perpetrare reati presupposto anche di altra natura.

In conformità alla Legge 90/2024, la Società ha rafforzato i protocolli di monitoraggio sugli accessi privilegiati. Ogni tentativo di accesso non autorizzato o alterazione di dati sarà perseguito non solo come violazione disciplinare, ma anche come potenziale reato presupposto aggravato se diretto a infrastrutture critiche

Per la definizione di misure organizzative adeguate a contrastare il perpetrarsi di reati presupposto l'Ente ha fatto ricorso ai seguenti principi guida:

- **Sistema di responsabilità/deleghe**: le responsabilità di gestione, coordinamento e controllo all'interno dell'azienda, nonché i livelli di dipendenza gerarchica e la descrizione delle relative responsabilità sono stati definiti e formalizzati in espliciti atti.
- **segregazione delle funzioni/attività**: nella struttura si è perseguita la separazione delle funzioni tra chi autorizza, chi esegue, chi registra, anche contabilmente, e chi controlla;

- **tracciabilità**: i processi di decisione, autorizzazione e svolgimento di ogni attività sensibile devono essere verificabili ex post, anche tramite appositi supporti documentali adeguatamente archiviati a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza.

Gli strumenti informatici, oltre che costituire un potenziale obiettivo di attacchi esterni o interni per il loro valore intrinseco e per le informazioni in essi contenute, possono costituire anche un mezzo per perpetrare reati di altra natura. Alcuni comportamenti possono comportare la responsabilità amministrativa dell'Ente ai sensi di quanto disposto dal D.Lgs. 231/01 ma altri sono altresì da evitare in quanto non in linea con i valori di cui al Codice Etico di cui l'Ente si è dotato.
Di seguito si riportano i principali comportamenti non tollerati e riscontrati anche grazie a controlli operati dall'Organismo di Vigilanza. L'Ente perseguirà severamente con sanzioni ed azioni a carico dei responsabili, le seguenti violazioni:

- cancellare o distruggere le registrazioni effettuate finalizzate alla documentazione delle attività in cui possono essere realizzati reati presupposto;
- introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza (615 ter C.P.);
- detenere e diffondere abusivamente codici di accesso a sistemi informatici o telematici (615 quater C.P.);
- diffondere, comunicare o consegnare programmi informatici aventi l'obiettivo di danneggiare un sistema informatico o telematico, nonché dati e programmi in esso contenuti (635 quater.1 C.P.);
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche nonché diffonderne il contenuto (617 quater C.P.);
- installare apparecchiature che hanno come finalità la realizzazione dei reati di cui al punto precedente (617 quinquies C.P.);
- danneggiare o distruggere informazioni, dati, programmi (635 bis C.P.) e sistemi (635 quater C.P.) anche utilizzati dallo Stato, da enti pubblici o di pubblica utilità (635 ter C.P., 635 quinquies);
- utilizzare il sistema informatico/telematico o attaccare un sistema informatico/telematico per perpetrare reati di natura estorsiva (629 C.P.);
- falsificare documenti informatici (491 bis C.P.);
- compiere frodi informatiche (640 ter C.P.);
- compiere o far compiere a minori atti che si possano qualificare come "prostituzione" (600 bis C.P.);
- realizzare, produrre materiale pornografico che vedano la presenza di minori o fornire indicazioni finalizzate all'adescamento o allo sfruttamento sessuale minorile (600 ter C.P.);
- detenere materiale pornografico di qualsiasi tipo ed, in particolar modo, materiale pornografico realizzato utilizzando minori (600 quater C.P.);
- realizzare, produrre, detenere materiale pornografico virtuale che abbia come protagonisti minori (600 quater bis C.P.);
- mettere a disposizione del pubblico mediante reti telematiche o connessioni di qualsivoglia genere opere d'ingegno protette o loro parti (171 c.1 lett. a-bis L. 633/41);

- duplicare programmi per elaboratore; importare, distribuire, vendere, detenere software non originale o programmi per dispositivi elettronici non originali. È altresì vietato, rimuovere o l'eludere dispositivi applicati a protezione di un software (171 bis L. 633/41);
- duplicare abusivamente, riprodurre, trasmettere e diffondere in pubblico opere dell'ingegno e banche dati (171 ter L. 633/41);
- produrre, vendere, importare, promuovere, installare, modificare fraudolentemente apparati atti alla decodifica di trasmissioni audiovisive ad accesso condizionato, effettuate anche via cavo in forma analogica o digitale (171 octies L. 633/41);
- adottare comportamenti di qualsiasi tipo svolti con strumenti di tipo elettronico non in linea con i valori aziendali.

3.2 Regolamento (UE) 2016/679 e D. Lgs. 196/03

La Direttiva normativa in materia di protezione dei dati personali è stata recepita nel nostro ordinamento con la L. 675 del 31/12/1996 che, successivamente, è stata abrogata e sostituita dal D.Lgs. 196 del 30/06/2003 - "*Codice in materia di protezione dei dati personali*". L'evoluzione tecnica e sociale ha imposto la necessità di aggiornare sia lo strumento che i contenuti delle disposizioni in materia di tutela dei dati personali: è stato, così, approvato il Regolamento (UE) 2016/679 (noto anche come "GDPR") che ha comportato la necessità di adeguare anche il D.Lgs. 196/03[3].
Acquedotto Poiana SpA si impegna ad applicare ed a far applicare, in modo rigoroso, da tutti i collaboratori a vario titolo, nonché dei business partner, la legislazione in materia di protezione dei dati personali, nel rispetto dei principi di Liceità, Correttezza, Trasparenza, Limitazione della finalità, Minimizzazione dei dati,
Esattezza, Limitazione della Conservazione, Integrità e riservatezza.
Tali principi sono ben descritti nella parte speciale "*Reati Informatici, reati contro la persona e violazioni del Diritto d'Autore*" di cui il presente documento costituisce un allegato operativo.

3.3 Pornografia e pedopornografia

L'Ente tutela con ogni mezzo i minori ed i diritti dell'infanzia. A tal fine privilegia rapporti di fornitura e subfornitura con soggetti che dichiarano di non avvalersi di minori per la produzione di beni e servizi.
Inoltre, perseguirà duramente la detenzione di materiale pedopornografico da parte di propri collaboratori o collaboratori dei propri business partener: ciò significa che non saranno tollerati la visualizzazione, il download o l'upload, lo scambio, la detenzione, la commercializzazione e l'archiviazione di materiale di contenuto pornografico e/o pedopornografico.
Non saranno tollerati, altresì, comportamenti finalizzati ad indurre minori ad avere comportamenti sessualmente espliciti od a scambiare foto, disegni, file multimediali con contenuti afferibili alla sfera sessuale di minori o per il loro adescamento.
L'ente si adopererà per censurare e contrastare con la massima determinazione comportamenti di questo tipo adottati da chiunque collabori con l'Ente.

[3] Ciò e avvenuto con il D.Lgs. 101/2018.

3.4 Diritto d'Autore

Acquedotto Poiana SpA è sensibile ai temi della protezione del diritto di Autore, oggi facilmente eludibile grazie al Web. Nell'ambito dei sistemi informatici, queste violazioni possono facilmente concretizzarsi attraverso:

- l'installazione di software non originale;
- l'utilizzo di un numero di copie di prodotti software maggiore rispetto al numero consentito dalla licenza (*underlicensing*) o dalle licenze disponibili;
- l'accesso non autorizzato a banche dati pubbliche;
- l'upload ed il download di file multimediali o l'accesso a piattaforme di utilizzo di materiale multimediale online.

Posto che è fatto divieto di utilizzare qualsiasi software se non autorizzato dall'Ente, sono vietati, altresì, tutti i comportamenti che violano i diritti l'autore e la proprietà intellettuale, anche se per finalità personale.
E' vietato, in particolare:

- detenere supporti di memorizzazione (DVD, HD esterni o altri supporti) che contengano materiale che viola la proprietà intellettuale;
- utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare, rimuovere protezioni, sproteggere ogni tipo di contenuto digitale;
- distribuire, diffondere, scambiare, condividere o modificare in ogni modo contenuti multimediali in violazione della licenza;
- duplicare file, archivi e contenuti multimediali.

Questi comportamenti sono prescritti anche a tutti coloro che collaborano, a vario titolo, con Acquedotto Poiana SpA e, pertanto, vanno prontamente segnalati all'OdV tutti i comportamenti che si configurino quali violazioni di quanto sopra prescritto, nel rispetto delle policy sul Whistleblowing e del Codice Etico.

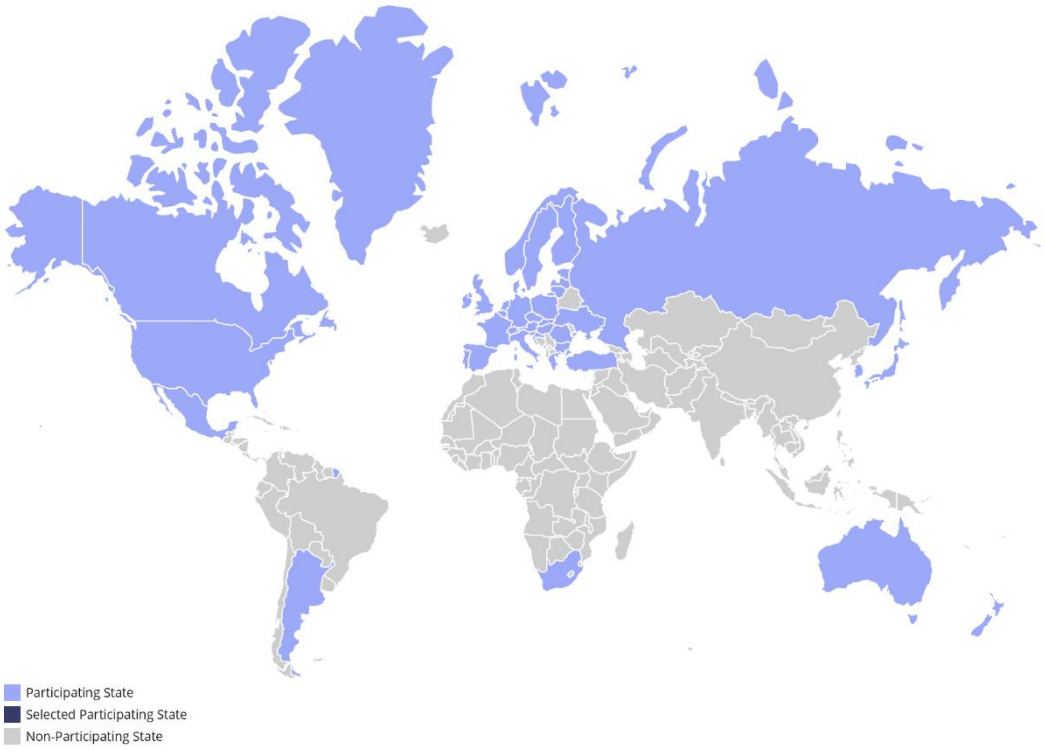
3.5 Social media

I collaboratori ed i partner che intendono utilizzare i social networks (Twitter, Youtube, Facebook,…) per conto di Acquedotto Poiana SpA devono essere autorizzati esplicitamente. Nell'intervenire in maniera pubblica in ambito professionale si deve tenere sempre presente che si sta agendo in nome e per conto di Acquedotto Poiana SpA e che, quindi, vanno evitate polemiche, prese di posizioni, comportamenti, discussioni quando queste possano essere espressioni di opinioni personali o di valori che Acquedotto Poiana SpA non condivide e non ha fatto propri, sia che abbiano ad oggetto direttamente Acquedotto Poiana SpA che soggetti diversi.
E' proibito divulgare sui social media notizie ed informazioni riservate afferenti la gestione strategica ed operativa di Acquedotto Poiana SpA, a meno che non vi sia un'esplicita autorizzazione. E', altresì, proibito pubblicare contenuti o link a contenuti in violazione del diritto di autore, della privacy e di ogni altra Legge nazionale od internazionale.
Anche qualora si intervenga sui Social Network con profili personali privati è opportuno tenere presente che qualsiasi informazione personale si riveli sui social networks di sé o dei propri colleghi può essere associata al nome di Acquedotto Poiana SpA e comprometterne la reputazione. Anche

se le opinioni che si esprimono sono personali, è bene tenere conto che parlare male di chiunque ha sempre conseguenze negative sia per chi esprime apertamente queste opinioni che per Acquedotto Poiana SpA. Sono altamente scoraggiati i battibecchi e le invettive e si raccomanda di applicare buon senso e professionalità.
E' bene tenere presente che tutto ciò che si pubblica su Internet rischia di essere permanente e può essere rintracciato dai motori di ricerca in ogni sua singola parola anche molti anni dopo la pubblicazione. Anche se apparentemente innocui, certi comportamenti e/o opinioni espresse possono creare problemi di immagine ed esporre ad attacchi, ricatti e pressioni che possono minare la libertà e la professionalità.

3.6 Attività in Paesi Esteri

Tutte le volte che un collaboratore diretto di Acquedotto Poiana SpA o di un outsourcer, si trovi ad utilizzare all'estero dispositivi o strutture che trattano dati aziendali di Acquedotto Poiana SpA, deve informarsi circa eventuali disposti di Legge del Paese interessato.
In particolare, si ricorda che prassi tollerate - se non addirittura incoraggiate - in alcuni Paesi possono risultare del tutto problematiche in altri. A titolo di esempio si precisa che la crittografia di alcuni device come laptop o smarphone non è legale in alcuni Paesi (Russia, Ukraina, …) e può portare al sequestro ed alla confisca degli stessi. Si prescrive, in questo caso, di verificare se il Paese estero è un firmatario dell'Accordo Wassenaar[4] (http://www.wassenaar.org/) che consente l'uso di dispositivi criptati a particolari condizioni.
La figura che segue mostra i Paesi che aderiscono all'Accordo Wassenaar.



[4] L'accordo è stato oggetto di modifiche nel 2023.

In maniera analoga, è prescritto a tutti color che intendono utilizzare i device all'estero di condurre un'analisi e produrre un report con le risultanze dell'approfondimento che deve essere trasmesso al Delegato.

4 Istruzioni Generali per l'utilizzo degli strumenti e dei servizi.

Gli Strumenti Informatici sono affidati a ciascun Utente, che deve custodirli con cura e deve tempestivamente informare il Delegato in caso di qualsiasi uso non autorizzato delle proprie credenziali di autenticazione, accesso non autorizzato, violazione della sicurezza, ovvero ogni altro incidente che coinvolga gli Strumenti assegnati. All'atto della consegna degli Strumenti Informatici, l'Utente dovrà sottoscrivere per ricevuta un apposito documento (***Allegato A***).

È Responsabilità del Delegato, attraverso il Referente Informatico, creare e mantenere sempre aggiornato l'elenco dei dispositivi ed accessori affidati agli Utenti, avendo cura di indicarne anche le caratteristiche ed i privilegi di utilizzo. Tale elenco dovrà essere direttamente consultabile dalla Direzione Aziendale e dall'Ufficio del Personale.

L'Utente deve provvedere all'eliminazione di ogni informazione personale dagli Strumenti Informatici, eventualmente memorizzata anche in violazione di quanto previsto dal presente Disciplinare, prima della restituzione degli stessi, sia in caso di sostituzione per rinnovo tecnologico, sia in caso di cessazione del rapporto di lavoro per qualsiasi causa. All'atto della restituzione, l'Utente dovrà firmare l'atto di riconsegna, patre integrante dell'*Allegato A*.

Gli Utenti devono prestare particolare cura alla custodia e conservazione degli Strumenti assegnati, soprattutto se portatili, onde evitare che vengano rubati, smarriti o danneggiati. Si raccomanda di non lasciare i dispositivi incustoditi durante viaggi e/o trasferte (a mero titolo esemplificativo, nei viaggi in aereo, non imbarcare i dispositivi nella stiva e, nei viaggi in auto, non lasciare i dispositivi all'interno del veicolo, anche se nascosti alla vista). La perdita dei dispositivi, oltre al loro valore intrinseco, può provocare la perdita di informazioni importanti per Acquedotto Poiana SpA, e quindi costituisce sempre un danno economico per questi ultimi nonché potrebbe determinare un data breach che, in alcuni casi, deve essere notificato all'Autorità Garante.
Gli Utenti devono, inoltre, bloccare l'utilizzabilità degli strumenti, bloccandoli, effettuando il log off o attivando lo screen saver protetto da password prima di allontanarsi, anche per brevi assenze.

In caso di furto o smarrimento di un dispositivo assegnato, l'Utente deve comunicare immediatamente (e comunque entro 24 ore) l'accaduto al Delegato - in modo che possa intervenire per adottare tutte le misure necessarie. L'Utente, ove il furto o lo smarrimento avvenga fuori dal luogo di lavoro, dovrà, inoltre, denunciare l'accaduto alle competenti autorità di Pubblica Sicurezza. Copia della denuncia deve essere consegnata entro tre giorni di calendario dall'evento al Delegato.

Gli Utenti non possono modificare le impostazioni degli Strumenti Informatici in dotazione né installare autonomamente periferiche o software ed app. E' altresì, vietato:

- avviare il personal computer con sistemi operativi diversi da quello installato incluse versioni live;

- utilizzare strumenti software e/o hardware atti ad intercettare, falsificare o alterare il contenuto di documenti informatici (a titolo esemplificativo, programmi di recovery password, cracking, sniffing, spoofing, serial codes);
- fare copia (diversa da quella di backup effettuata secondo le procedure aziendali) dei software installati o di documenti. La copia dei documenti è consentita solo se necessaria allo svolgimento dell'attività lavorativa;
- creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare sistemi informatici quali per esempio virus, trojan horses, ecc.;

Gli Utenti sono tenuti a dare tempestiva segnalazione di eventuali anomalie o irregolarità nel funzionamento degli Strumenti Informatici assegnati, al fine di prevenire la perdita totale o parziale della riservatezza, integrità o disponibilità delle informazioni in essi contenute nonché di evitare eventuali guasti all'intero sistema.

L'assegnazione degli Strumenti Informatici potrà essere revocata in caso di uso improprio da parte dell'Utente. Anche in questo caso (indipendentemente dal motivo di tale richiesta), gli Strumenti Informatici dovranno essere restituiti al Delegato nella loro integrità, comprese eventuali periferiche interne ed esterne.

Si ricorda che le unità di memorizzazione locale (es. disco C: o Desktop) non devono essere utilizzate per salvare documenti frutto dell'attività lavorativa in quanto non sono soggette alle politiche di backup dati aziendali gestito dal Servizio Sistemi Informativi.

5 Sicurezza dei dati e dei sistemi.

L'informazione è un bene che, al pari di altri beni che costituiscono il patrimonio di un'azienda o di un ente, rappresenta un valore per l'organizzazione e necessita, pertanto, si essere adeguatamente protetto. Qualunque forma assuma e qualunque siano i mezzi con cui vengono condivise e memorizzate, vanno sempre adeguatamente protette, ovvero debbono essere assicurate:

- **riservatezza** ("*confidentiality")*: nessun utente interno o esterno e nessun processo deve aver la possibilità di ottenere o dedurre dal sistema informazioni che non è autorizzato a conoscere;
- **integrità** ("*integrity*"): il sistema deve impedire (e, comunque, rilevare) le azioni atte ad alterare le informazioni sia da parte di utenti che di processi non autorizzati o a causa di eventi accidentali;
- **disponibilità** ("*availability*"): il sistema deve garantire la disponibilità a ciascun utente o processo autorizzato ad accedere alle informazioni nei tempi e nei modi prestabiliti;
- **autenticità** ("a*uthenticity*"): il sistema deve garantire la provenienza certa di un'informazione;
- **non ripudio** ("*non repudiation*"): il sistema deve essere in grado di garantire le informazioni da falsa negazione di ricezione, trasmissione, creazione, trasporto, consegna e ricezione di un'informazione.

Al di là delle premesse generali, il Regolamento (UE) 2016/679 definisce il concetto di "**sicurezza**" avendo riguardo, specificatamente, la riservatezza, l'integrità, la disponibilità e la resilienza:

Art. 32
Obblighi di sicurezza

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Il concetto di Resilienza è un'importante passo avanti nella gestione della sicurezza perché, posto che è ineludibile essere oggetto di attacchi, il sistema deve essere configurato in modo da recuperare l'operatività e rispondere, anche adattandosi, ad un attacco informatico.

Quanto sopra riportato costituisce logica premessa per, poi, comprendere come le contromisure constino di iniziative di natura tecnica, organizzativa e procedurale e che, quindi, il comportamento degli utenti e dei collaboratori in genere contribuisca alla sicurezza del sistema. Di qui, la necessità di adottare delle policy che permettano di individuare la correttezza dei comportamenti per la piena sicurezza del trattamento dati attraverso un corretto utilizzo degli strumenti a disposizione.

5.1 Collaboratori ed utilizzo del sistema informativo e dei dati

Acquedotto Poiana SpA si è dotato di un sistema di autorizzazione: ogni soggetto che necessita di trattare dati ed utilizzare il sistema informativo deve essere associato ad uno o più profili che definiscono, quali dati ciascun soggetto può trattare e quali operazioni può compiere sui dati.
Il profilo di autorizzazione viene definito compiutamente nella nomina ad Autorizzato che andrà sottoscritta per accettazione dal destinatario o nel contratto sotteso alla prestazione dell'Outsourcer.

A seguito di una cessazione del rapporto lavorativo o di consulenza con Acquedotto Poiana SpA o, comunque, al venir meno, ad insindacabile giudizio dell'ente, della permanenza dei presupposti per l'utilizzo di device aziendali o del rapporto di collaborazione, i collaboratori hanno i seguenti obblighi:

- Procedere immediatamente alla restituzione dei device in uso;
- Divieto assoluto di formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo;
- Procedere immediatamente alla restituzione dei dati cartacei in loro possesso;
- Divieto assoluto di alterare o manomettere o distruggere i documenti cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.

5.2 Credenziali di Autenticazione.

Il trattamento di dati, in particolare di dati personali, con strumenti elettronici è consentito ai soli soggetti dotati di credenziali di autenticazione, costituite da dati o da dispositivi, in possesso esclusivo di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per la verifica, anche indiretta, dell'identità.
L'incaricato dovrà adottare le necessarie cautele per assicurare la segretezza della componente riservata delle credenziali e la diligente custodia dei dispositivi in suo possesso ed uso esclusivo.
In particolare, le password non dovranno essere annotate su supporti posti in prossimità del computer e dovranno essere custodite adeguatamente, così come i token o le chiavi di accesso a locali ad accesso selezionato e non debbono essere lasciati incustoditi.

Le password iniziali sono previste ed attribuite dal **Referente Informatico** ma all'atto del primo utilizzo, ciascun utente è tenuto a modificarle. È garantita, anche, l'autonoma sostituzione da parte dei singoli utenti ogni qualvolta lo ritengano opportuno e, comunque, ogni tre mesi (se trattano dati particolari e/o giudiziari) o sei mesi (dati comuni).
Per le password, valgono i seguenti accorgimenti:

- Deve essere di lunghezza non inferiore a 8 caratteri oppure, nel caso in cui ciò non sia possibile, di un numero di caratteri pari al massimo consentito (ad esempio nel caso di cellulari, smartphone e tablet);
- Non deve contenere riferimenti agevolmente riconducibili all'autorizzato o essere di facile individuazione.
- Non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere), tratta da informazioni personali.
- Non deve presentare una sequenza di caratteri identici o in gruppi di caratteri ripetuti.

- Per essere maggiormente efficace deve essere composta da caratteri maiuscoli, minuscoli, da numeri e caratteri speciali (per esempio ?E21s3tHi%).
- Deve essere diversa da quelle utilizzate in precedenza.
- Deve essere nota esclusivamente all'utilizzatore e non può essere assegnata e/o comunicata ad altri.
- Non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet.

E' assolutamente proibito entrare nella rete od utilizzare programmi utilizzando le credenziali di autenticazione di un altro utente.
La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza.
Chi venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al **Referente Informatico**.
In caso di assenza prolungata di un utente, il Titolare può provvedere ad assegnare ad altri soggetti, permessi di accesso al trattamento dati o permessi di utilizzo dei dispositivi.
A tale fine il **Referente Informatico** potrà richiedere all'assegnatario la comunicazione della password, la consegna dei dispositivi ad uso esclusivo, o potrà procedere al resetting della password in utilizzo al collaboratore.
Le comunicazioni, le operazioni e le scelte effettuate saranno oggetto, a cura del **Referente Informatico**, di apposito verbale, trasmesso in copia all'utente con modalità tali da attestare l'avvenuta ricezione e conservato in originale presso la sede di Acquedotto Poiana SpA.
Una copia delle credenziali di autenticazione con i privilegi di amministratore di sistema relativamente a ogni componente del sistema informativo dovrà essere custodita in busta chiusa in un luogo sicuro.
Non è consentita l'attivazione di credenziali di protezione autonome (ad esempio, password di protezione delle cartelle) senza preventiva autorizzazione da parte del **Referente Informatico**.
Le credenziali che non vengono utilizzate da parte degli assegnatari per un periodo superiore ai sei mesi verranno disattivate.

5.3 Supporti magnetici o cartacei: utilizzo, riutilizzo e loro dismissione.

Tutti i supporti magnetici riutilizzabili o rimovibili (DVD, HD esterni, cassette, chiavette USB, …) contenenti dati devono essere gestiti con particolare cautela, onde evitare che il loro contenuto possa essere conosciuto anche da parte di soggetti non autorizzati. La loro dismissione deve avvenire per distruzione fisica o per cancellazione sicura mediante programmi di file shredding o file erasing.
Anche i documenti cartacei (stampe e fax) contenenti dati personali o dati aziendali riservati debbono essere trattati nel "distruggi documenti" se non più utili e destinati alla dismissione.
E' vietato il riutilizzo anche come di fogli di brutta o per stampe di prova di fogli contenenti dati personali.
La dismissione di sistemi di trattamento quali pc, smartphone e altri deve essere preceduta dalla cancellazione sicura dei dati contenuti e dalla rimozione delle credenziali di accesso eventualmente memorizzate.

5.4 Protezione antivirus.

Ogni utente deve tenere comportamenti tali da ridurre il rischio di un attacco malware al sistema informatico aziendale.
A tal fine, ogni utente deve prestare la massima attenzione ai supporti di origine esterna (DVD, chiavette USB, HD, …), al download di file da internet o quali allegati di posta elettronica, preoccupandosi di effettuare una scansione antivirus prima della loro apertura. É necessario diffidare dei file allegati con estensione del nome tipo EXE, COM, VBS, così come di tutti quelli che presentano una doppia "falsa" estensione (come ad esempio "VIDEO.AVI.VBS").
In Acquedotto Poiana SpA è presente un sistema Antivirus centralizzato, con aggiornamento giornaliero delle definizioni di virus ed analisi periodica del sistema. É necessario quindi verificare che vicino all'orologio della barra di avvio di Windows (posizione standard: in basso a destra osservando il monitor), sia sempre presente l'icona dell'antivirus; controlli analoghi andranno effettuati in caso di dispositivi dotati di differenti sistemi operativi.
Nel caso che il software antivirus rilevi la presenza di un virus nel sistema o nei supporti rimovibili, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- segnalare immediatamente l'accaduto al **Referente Informatico**.

Il sistema di protezione antivirus memorizzerà per un periodo i 3 mesi ogni evento potenzialmente pericoloso per il sistema informatico, evidenziando il file infetto, nonché l'utente che vi ha avuto accesso.
Per ridurre la possibilità di infezioni virali, è data facoltà al Titolare di disabilitare lettori, porte USB, e di impedire l'installazione di programmi agli utenti.

5.5 Firewall

I confini del Sistema Informatico di Acquedotto Poiana SpA sono protetti da un Firewall che blocca il traffico non consentito da e verso l'esterno, inviando un alert ai soggetti deputati al controllo (**Referente Informatico**, in primis) in caso di accessi a siti non ammessi, di utilizzo di software non ammesso ed in caso di eventuale traffico dati non usuale.
La presenza del Firewall non preclude l'accesso al sistema dall'esterno: a tutti gli utenti che lo richiedono per esigenze lavorative è permesso di accedere in modalità SSL VPN ad alcune risorse aziendali ben specificate.
E' possibile, per il **Referente Informatico**, definire in quali fasce orarie ed a quali dati ciascun utente può accedere in funzione del ruolo e delle mansioni assegnategli.

5.6 Sistemi di Mobile Device Management (MDM)

Per tutti i dispositivi mobile assegnati in uso, essendo strumenti di lavoro, valgono le medesime indicazioni previste per i computer ed i laptop in ordine ai reati di matrice pedopornografica e/o relativi al copyright.
Le telefonate personali durante l'orario di lavoro, sia da telefono fisso sia da cellulare, devono essere ridotte al minimo indispensabile e non devono interferire in alcun modo con il normale svolgimento della propria attività lavorativa o quella dei colleghi.
Gli apparecchi forniti potrebbero essere utilizzati anche per il trattamento di dati personali di cui Acquedotto Poiana SpA è titolare (foto, filmati, mail e documenti) e, pertanto, vanno conservati con

cura, adottando protezioni attive degli accessi al loro contenuto (password di sblocco, screen saver ,…). Per essi valgono le medesime cautele previste per i pc portatili.

Acquedotto Poiana SpA si riserva di effettuare controlli sull'utilizzo dei cellulari aziendali al fine di analizzare l'andamento complessivo dei consumi in modo da valutare nel tempo l'adeguatezza del contratto con il provider di fonia e traffico dati, con l'obiettivo di ridurre i costi aziendali e ottimizzare la qualità del servizio nonché rilevare eventuali situazioni anomale di consumi.
Acquedotto Poiana SpA, pertanto, si riserva di verificare i dati di traffico generato dalla sim abbinata allo smartphone aziendale. I dati ricevuti dal fornitore del servizio di comunicazione elettronica riportano i numeri chiamati con mascheramento delle ultime 3 cifre. I controlli verranno effettuati dal **Referente Informatico**.
Al fine di garantire la sicurezza degli apparati, Acquedotto Poiana SpA si riserva la possibilità di installare e attivare sui dispositivi mobile (cellulari tradizionali, smartphone, tablet) un sistema di gestione che consente di migliorare la sicurezza:

- Impedendo l'installazione di app se non a livello centrale;
- Bloccando il dispositivo in caso di furto o smarrimento;
- Garantendo la possibilità di un pieno reset del dispositivo;
- Consentendo eventuali backup.

Non vengono attivati processi di geolocalizzazione degli apparati.
Stante il possibile controllo sull'operato del dipendente, soluzioni MDM sono effettuate nel rispetto dell'art. 4 della L.300/70.

5.7 Politiche di backup

Il backup delle cartelle personali ubicate sul server è automatico. Eventuali file salvati sui dispositivi personali non sono oggetto di backup salvo esplicita richiesta in tal senso da parte del responsabile di settore. Quest'ultimo può anche richiedere tempi di retention differenti in funzione di obblighi di legge o per esigenze operative.
Per il restore di file eventualmente cancellati è possibile rivolgersi al **Referente Informatico** che intraprenderà i provvedimenti del caso.

5.8 Patching

Il patching (ovvero l'installazione di software o firmware che risolve problemi di funzionamento dei dispositivi) è automatico in rete per i PC ed i laptop mentre avviene in maniera manuale per smartphone e tablet.

6 Posta elettronica e Internet.

Il presente paragrafo prende lo spunto dalle linee guida elaborate dall'Autorità Garante italiana con il Provvedimento a carattere generale del 01/03/2007[5]. L'Autorità, proprio con il fine di tutelare i legittimi interessi di dipendenti senza penalizzare i datori di lavoro, ha inteso elaborare un

[5] Il provvedimento è stato pubblicato in G.U. n. 58 del 10 marzo 2007

documento che riporta alcune osservazioni e puntualizzazioni al fine di assicurare *"la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati […], in una cornice di reciproci diritti e doveri"* nonché *"l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali".*

Si deve, comunque, partire da alcune premesse:

a) compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;

b) spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;

c) emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;

d) l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

Tutto ciò premesso, Acquedotto Poiana SpA ritiene di dover disciplinare l'utilizzo della posta elettronica e l'accesso ad Internet e, qualora si evidenzi che la posta elettronica e la rete Internet vengono utilizzate indebitamente, Acquedotto Poiana SpA si riserva di perseguire il collaboratore dal punto di vista disciplinare.

6.1 Internet

Il PC abilitato alla navigazione in Internet costituisce, al pari delle atre dotazioni, uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. Ne consegue che è assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

A tale fine è stato attivato un sistema di *content filtering* che prevede una black list di siti non accessibili agli utenti.

Chiunque, per finalità legate allo svolgimento delle proprie mansioni, necessiti di accedere ad uno dei siti bloccati dl sistema di content filtering può richiedere lo sblocco dell'accesso, indirizzando una richiesta in tal senso al **Referente Informatico.**

Mediante l'utilizzo di sistemi aziendali, è vietata la partecipazione non autorizzata a Forum anche se professionali, l'utilizzo di Chat line (esclusi gli strumenti autorizzati), la consultazione di social networking come Facebook, Instagram, Twitter ed altri, nonché l'uso di bacheche elettroniche.
E', altresì, vietato l'utilizzo dei dispositivi informatici aziendali per l'accesso a webmail extra-lavorative anche se effettuato fuori dall'orario di lavoro o durante le pause.
E' vietato visitare siti di hacking ed è vietato anche ascoltare stazioni radio o televisive in modalità streaming continuo.

Nonostante i divieti, non verranno raccolti in maniera occulta per finalità relative al controllo dei dipendenti né dati relativi alle pagine web visitate dal collaboratore, né file temporanei, né cookies che non siano di natura tecnica.

6.2 Posta Elettronica ed indirizzi mail aziendali.

La casella di posta assegnata all'utente da Acquedotto Poiana SpA è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse e, quindi, è precluso l'utilizzo indiscriminato delle caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing list, salvo diversa ed esplicita autorizzazione.
E' tuttavia, tollerato un limitato utilizzo della posta per finalità personali ma, in tale evenienza, l'Utente deve:

- contrassegnare nell'oggetto la corrispondenza in modo tale da evidenziarne il contenuto riservato (per esempio, inserendo nell'oggetto "Personale" o "Riservato";
- rimuovere dal testo ogni elemento riconducibile ad Acquedotto Poiana SpA e che possa far intendere che il messaggio è inviato nello svolgimento della propria attività lavorativa;
- conservare tale corrispondenza per il tempo strettamente necessario, provvedendo ad eliminarla quanto prima.

Potranno essere attivati indirizzi a disposizione di più incaricati (ad esempio, amministrazione@poiana.it, ...).
In caso di assenza, è fatto obbligo di attivare il sistema di risposta automatica che indica le coordinate di un altro soggetto cui rivolgersi per urgenze. In caso di inottemperanza da parte dell'incaricato o nella concreta possibilità che quest'ultimo non possa provvedere per cause di forza maggiore, tale sistema potrà essere attivato dal Titolare per tramite del **Referente Informatico**, dandone comunicazione all'incaricato mediante sistemi che consentano l'accertamento dell'avvenuta ricezione (raccomandata A/R, posta elettronica certificata, …).
Ogni messaggio di posta elettronica dovrà recare un *disclaimer* che, in aggiunta alle normali indicazioni sul rispetto della privacy, riporti che i contenuti dei messaggi che devono avere natura aziendale e potranno essere conosciuti nell'ambito dell'organizzazione con le modalità individuate nella presente policy aziendale.
A titolo di esempio:

> *"**NATURA AZIENDALE DEL MESSAGGIO E NOTE DI RISERVATEZZA***
> *Il presente messaggio ha contenuto aziendale e non personale, da cui discende, come indicato nella policy aziendale, **la possibilità che sia conosciuto nell'ambito dell'organizzazione e non unicamente dal destinatario**.*

Le informazioni in esso contenute sono da considerarsi strettamente riservate ed il loro utilizzo è destinato esclusivamente dall'Organizzazione destinataria. Le informazioni potrebbero essere oggetto di privilegio o altra norma a tutela della riservatezza. Chi legge questo messaggio senza averne titolo è consapevole che trattenere la stessa, divulgarla, distribuirla a persone diverse dal destinatario o farne copia è severamente proibito. Qualora riceveste questo messaggio per errore, siete pregati cancellarlo e di darcene comunicazione."

Stante la loro potenziale pericolosità, il sistema automaticamente sottoporrà a scansione gli allegati ai messaggi di posta elettronica prima della loro apertura. Una volta scaricati, i messaggi di posta elettronica vengono cancellati dal mail server: la casella di posta personale deve essere mantenuta in ordine, cancellando documenti inutili e, soprattutto, allegati ingombranti non necessari.
E' vietato dar seguito alle catene telematiche (Hoax) e, se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al **Referente Informatico** e non si deve in alcun caso, aprire gli allegati a tali messaggi.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o pre-contrattuali ovvero contenga documenti da considerarsi riservati deve essere visionata ed autorizzata in ossequio ai poteri di firma definiti da Acquedotto Poiana SpA. Messaggi contenenti dati personali particolari di cui all'art 9 del Regolamento (UE) 2016/679 ("GDPR") o dati giudiziari, debbono necessariamente essere crittografati.
Benchè sia possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, è prescritta l'adozione, di strumenti tradizionali (raccomandate A/R) o della posta elettronica certificata per l'assunzione di impegni contrattuali.
Per ciò che attiene il salvataggio dei messaggi di posta elettronica, la struttura garantisce il salvataggio dei messaggi non ancora scaricati dal Mail Server. Una volta scaricati, i dati contenuti nei messaggi sono archiviati sui PC degli utenti e saranno salvati solo su esplicita richiesta dell'incaricato, con modalità e tempistiche da definire.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Al fine di garantire il corretto funzionamento della posta elettronica aziendale e di evitare la proliferazione del traffico indebito (spam), Acquedotto Poiana SpA si è dotata di un sistema antispam.

Le caselle di posta individuali hanno validità pari alla durata della permanenza del rapporto con Acquedotto Poiana SpA da parte dell'Utente. Nel caso in cui il rapporto di interrompa, la casella di posta elettronica sarà immediatamente disattivata con contestuale adozione di sistemi automatici volti a fornire al mittente indirizzi alternativi che possono essere contattati per garantire la continuità aziendale. Il messaggio automatico di risposta avrà il seguente tenore:

"Il presente account di posta è stato disattivato ed è quindi inibita la ricezione in entrata dei messaggi. Tutte le mail professionali precedentemente indirizzate a questo indirizzo dovranno essere inviate al seguente indirizzo _____".

6.3 Il Rapporto fra Outsourcer, Fornitori e Acquedotto Poiana SpA

Ogni volta che viene stabilito un contratto di fornitura di servizi e/o di outsourcing, deve essere privilegiato un certo grado di formalità. In particolare, debbono essere definiti in sede contrattuale (disciplinare di appalto o capitolato di fornitura) alcuni aspetti quali:

- gli ambiti di fornitura (costi, tempi e Service Level Agreement) nonchè le caratteristiche del prodotto/servizio oggetto della fornitura stessa;
- gli ambiti di operatività consentiti, i tempi di revisione e di scadenza;
- eventuali restrizioni alla copia, alla rivelazione o all'utilizzo di informazioni ed accordi di riservatezza (Non Disclosure Agreements - NDA);
- training e coaching richiesto nei confronti dei collaboratori;
- controlli per la protezione dal malicious code;
- accorgimenti per eventuali investigazioni in occasione di incidenti di sicurezza o in caso di commissione di reati presupposto di cui al D.Lgs. 231/01;
- possibilità per Acquedotto Poiana SpA di monitorare gli aspetti contrattuali anche ricorrendo ad auditing di terze parti, presso la propria sede o altrove, nonché possibilità di revocare permessi di accesso agli asset aziendali;
- diritti di proprietà intellettuale;
- possibilità o impossibilità e condizioni per un eventuale subcontracting;
- condizioni per una revisione degli accordi ed accorgimenti in caso di rottura contrattuale od in caso l'outsourcer non sia in grado di fornire i beni/servizi con gli SLA richiesti;
- responsabilità per l'implementazione degli accorgimenti prescritti agli amministratori di sistema;
- impegno a considerare vietato tutto ciò che non è esplicitamente permesso;
- controlli per assicurare che i dati e le informazioni non siano utilizzate alla fine del rapporto o ad un momento contrattualmente prestabilito.
- impegno al rispetto del Codice Etico ed alle prescrizioni del Modello di Organizzazione Gestione e Controllo dell'Ente.

Ogniqualvolta un soggetto esterno venga chiamato a svolgere un servizio per conto di Acquedotto Poiana SpA, oltre a definire con chiarezza i termini del contratto, il responsabile della funzione entro i confini della quale si svolge la prestazione di servizi, dovrà preoccuparsi di definire anche le necessità di accesso a dati e sistemi di Acquedotto Poiana SpA. A tal fine, dovrà preoccuparsi di riempire il modulo "**Allegato B"**, appositamente predisposto, che disciplina, a seconda dei casi:

- l'eventuale accesso fisico alla struttura (uffici, sala server, …);
- l'eventuale accesso logico;
- il tipo di connettività tra l'outsourcer e Acquedotto Poiana SpA;
- a quali dati e con quali permessi (R, W, X);
- se le informazioni ed i dati cui il fornitore ha accesso abbiano caratteristiche di confidenzialità;
- se vi siano informazioni che non possono essere conosciute dall'outsourcer e quali controlli (implementati o da implementare) consentano la protezione;
- come identificare il personale afferente l'outsourcer in occasione del trattamento (ad es. Cartellino identificativo, badge, …);

- l'impatto di un'eventuale indisponibilità all'accesso di terze parti, nonché le conseguenze di un dato errato o di un inserimento errato da parte o subito dall'outsourcer;
- eventuali requisiti legali e/o clausole contrattuali o regolamentari di cui tener conto;
- se i collaboratori dell'outsourcer rivestano il ruolo di amministratore di sistema secondo il Provvedimento dell'Autorità Garante italiana del 27/11/2008;

In base a quanto individuato, sarà anche necessario provvedere a qualificare il rapporto con il Titolare del trattamento: in altri termini il Titolare deve decidere sul ruolo del collaboratore e/o sulla natura e la tipologia dell'interdipendenza fra il soggetto esterno e Acquedotto Poiana SpA, nominando "Autorizzato" ogni collaboratore dell'Outsourcer ovvero qualificare quest'ultimo quale "Responsabile del Trattamento" o verificare se sussistano gli estremi per una contitolarità piuttosto che per una "Titolarità autonoma del Trattamento".
Questo tipo di comportamento va tenuto nei confronti di tutti gli outsourcer, tra cui anche i service provider (ISP, Network Provider, servizi telefonici), fornitori di servizi di sicurezza, consulenti di management e di business, sviluppatori e fornitori di SW e sistemi IT, soggetti che forniscono servizi di pulizia, di catering ma anche personale temporaneo (studenti, stagisti ed altro personale temporaneo).
Ogni soggetto interno che si trovi a gestire rapporti con soggetti esterni che trattino dati personali (outsourcer, fornitori di servizi, stagisti ed interinali) è tenuto a verificare l'eventuale presenza di una qualificazione del soggetto (Titolare autonomo, Contitolare, Responsabile o Autorizzato) garantendo il rispetto di quanto riportato nell'atto di qualificazione.
Qualora si notino figure estranee o non conosciute nell'ambito dell'organizzazione, è fatto obbligo di accertare l'identità di tali figure e, nel caso di accessi illegittimi o non autorizzati, è importante avvisare immediatamente i vertici della struttura che provvederanno alle verifiche del caso. Analogamente, anche qualora alcune figure operino fuori dall'ambito operativo consentito, i responsabili della struttura debbono essere prontamente avvisati.

6.4 Wireless Access Policy

L'accesso di un dispositivo alla rete wireless deve essere previamente autorizzato dal Delegato se il dispositivo deve operare trattamenti di dati ed informazioni aziendali. L'accesso può essere consentito solo a patto che il proprietario/affidatario garantisca e si impegni affinchè il dispositivo sia soggetto a misure di sicurezza che il Delegato, tramite il **Referente Informatico**, giudica compatibili con il trattamento dati cui è deputato.
La Struttura può anche dotarsi di una rete wireless scollegata dalla rete aziendale che fornisce unicamente connettività web, per la quale non sono previste forme particolari di tutela, se non quelle di identificare in maniera univoca l'utente in virtù del Codice Penale (che impone il concorso a chi offre un supporto alla commissione dei reati) o qualora i fornitori di connettività cui Acquedotto Poiana SpA si rivolge prevedano esplicitamente responsabilità a carico di quest'ultima.

6.5 BYOD presso Acquedotto Poiana SpA

La sigla BYOD, acronimo di "*Bring Your Own Device*" si riferisce al caso in cui i collaboratori o consulenti esterni utilizzano nell'attività lavorativa i propri dispositivi (laptop, smartphone, tablet,…) per l'accesso ai dati, strutture, device ed applicazioni della rete aziendale.

L'attenzione che viene riposta su questo argomento è facilmente comprensibile se si riflette che l'utilizzo di questi strumenti può compromettere la sicurezza e può portare, nel caso di trattamento di dati personali, a conseguenze anche penali per il Titolare del Trattamento.
Prendendo spunto dalla Guida redatta dall'Information Commissioner's Office , ogni volta che deve essere preso in considerazione l'utilizzo di una simile modalità operativa, in funzione del soggetto ammesso al BYOD, vanno chiariti:

- la tipologia e la natura dei dati trattati;
- il luogo di conservazione dei dati;
- le modalità di trasferimento e il flusso dei dati;
- le possibilità di perdita/alterazione dei dati;
- il livello di commistione/promiscuità tra finalità personali e aziendali nei trattamenti dei dati;
- il livello di sicurezza dei singoli dispositivi mobili;
- gli effetti di una potenziale conclusione del rapporto lavorativo tra Impresa e lavoratore;
- le modalità di gestione di eventuali perdite, furti, malfunzionamenti e/o rotture di un dispositivo.

Il principale problema connesso a questa pratica è da collegarsi al fatto che, sul dispositivo personale, vi è una promiscuità informativa e, inoltre, che debbono essere gestite questioni di sicurezza su dispositivi non di proprietà di Acquedotto Poiana SpA. Ciò si traduce, ad esempio, nella presenza in un unico archivio di email personali e lavorative, con la necessità di adottare soluzioni in grado di tutelare la privacy dell'interessato in caso di necessità di accesso.
Di qui la necessità di definire alcune caratteristiche minime di sicurezza sia fisiche, che logiche che procedurali precisate nel documento di assenso all'utilizzo di propri dispositivi che descriverà anche dove possono essere conservati i dati, come procedere al backup, frequenza e modalità di sincronizzazione.

6.6 Smart Working

L'evoluzione tecnologica e sociale hanno reso lo smart working una modalità operativa particolarmente diffusa che, di fatto, ha reso anche alcuni ambienti esterni al perimetro aziendale dei veri e propri luoghi di lavoro.
Le regole che vengono riportate qui di seguito, intendono prescrivere alcuni accorgimenti che consentono di mantenere alcuni aspetti di sicurezza legati al trattamento dati e sono stati elaborati anche alla luce del vademecum pubblicato dal Cert-Pa di AgId anche sulla base delle misure minime di sicurezza informatica per le pubbliche amministrazioni fissate dalla circolare 18 aprile 2017 , n. 2/2017 e delle raccomandazioni dell'ENISA, l'Agenzia europea per la sicurezza delle reti e dell'informazione, per smart working e telelavoro.

- Se possibile, vanno utilizzati dispositivi aziendali invece che personali.
- Se si utilizzano dispositivi personali, è obbligatorio che:
    - si utilizzino dispositivi che su cui siano presenti sistemi operativi per i quali attualmente è garantito il supporto;
    - si utilizzino dispositivi per i quali si è provveduto ad effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo;

- il dispositivo sia dotato di software di protezione (Firewall, Antivirus, Antimalware) abilitati e costantemente aggiornati;
- gli accessi al sistema operativo siano protetti da una password con almeno 8 caratteri o con un numero di caratteri pari al massimo consentito dal dispositivo;
- il dispositivo non sia accessibile a persone diverse dal collaboratore, nemmeno se è un familiare.

- Sui dispositivi utilizzati per questioni professionali non devono essere installati software illegali, provenienti da fonti/repository non ufficiali o in violazioni delle condizioni di licenza. I software debbono essere sempre aggiornati con l'installazione di tutte le patch previste dal produttore;
- Sui dispositivi utilizzati per questioni professionali, specialmente quando si ha a che fare con informazioni ed applicazioni critiche, è vietato svolgere sullo stesso dispositivo attività di smart working e attività personali:
- E obbligatorio collegarsi via Internet utilizzando una rete sicura. Vanno evitate reti aperte o gratuite;
- va evitato, per quanto possibile, lo scambio di informazioni critiche aziendali attraverso posta elettronica, smistata su reti non sicure;
- gli scambi di informazioni critiche debbono avvenire utilizzando una VPN o la rete intranet aziendale;
- i dati che vengono scaricati su supporti di memoria esterna devono essere sempre crittografati, come protezione da furto o perdita del supporto stesso;
- Deve essere sempre attivato lo screen saver protetto da password o bloccato l'accesso al dispositivo e/o configurata la modalità di blocco automatico quando si si allontana dalla postazione di lavoro;
- L'utente ha l'obbligo di segnalare immediatamente al Responsabile IT qualsiasi sospetto di attacco *Ransomware* (es. file non apribili o richieste di riscatto a video), al fine di mitigare la responsabilità dell'Ente ai sensi dell'art. 629 c.3 c.p.".

6.7 Archivi, dati e documenti.

Tutte le informazioni, gli studi, i documenti ed ogni altro elaborato, predisposti nell'esecuzione delle proprie mansioni o in esecuzione di una prestazione professionale o servizio svolto in outsourcing, sono di proprietà di Acquedotto Poiana SpA (salvo esplicito accordo in tal senso) e dovranno essere consegnati o riconsegnati non appena terminato l'incarico o, in pendenza di tale incarico, su semplice richiesta dei vertici della struttura.
I documenti per l'espletamento delle mansioni debbono essere riposti al sicuro al termine del proprio lavoro se gli archivi non sono ad accesso selezionato: eventuali documenti cartacei (fax, lettere, documenti scritti,…) non dovranno essere lasciati sugli apparecchi di ricezione, sparsi sulla scrivania o sulle mensole ma, piuttosto, prontamente rimossi e conservati in maniera ordinata e discreta.
Eventuali stampe contenenti dati personali, in particolar modo quelli «particolari» e/o relativi a condanne penali e reati, debbono essere prontamente ritirate da stampanti e/o fax, avendo cura di custodirne il contenuto.

Nell'ipotesi che i dati contenuti siano classificabili come «particolari» o possano determinare gravi conseguenze per l'interessato, i supporti magnetici, gli atti ed i documenti non presidiati debbono essere conservati in contenitori muniti di serratura fino alla restituzione.
Nelle conversazioni telefoniche o interne è indispensabile che non si faccia riferimento a dati personali riservati: le conversazioni delicate vanno effettuate in locali appositi. Deve essere prevenuta l'involontaria acquisizione di informazioni da parte di terzi attraverso un rigoroso rispetto della distanza di cortesia.
Le comunicazioni con gli interessati e, in particolar modo, con i lavoratori debbono essere individualizzate, adottando le misure più opportune per prevenire una indebita conoscenza da parte di soggetti terzi. Gli accorgimenti da utilizzare prevedono: la consegna in busta chiusa; il ritiro da parte dell'interessato o di un suo delegato che produca una delega scritta con firma originale dell'interessato; comunicazioni telematiche individuali.
Per il trattamento di dati sanitari, vanno adottate, in ragione della peculiarità dei dati stessi, alcune precauzioni: i dati anagrafici e di salute debbono essere trattati in forma disgiunta anche quando ci si riferisce a dati trattati in modalità diversa da quella telematica.
Quando si trattano i dati relativi alle assenze per malattia, ove i certificati di medici prodotti dal lavoratore siano redatti su modulistica diversa da quella appositamente predisposta e sul certificato predetto sia visibile oltre che la prognosi anche la diagnosi, è compito di chi opera il trattamento oscurare quest'ultima in modo che non sia assolutamente intellegibile e, comunque, far circolare i documenti, al pari di tutti gli altri contenenti dati sanitari, in busta chiusa.
In caso di denuncia all'INAIL è fatto obbligo di comunicare all'ente assistenziale esclusivamente le informazioni sanitarie relative alla patologia denunciata.
E' fatto esplicito divieto di utilizzo delle informazioni aziendali per fini personali o diversi da quelli afferenti con la propria mansione e con il proprio ruolo.
Senza autorizzazione non è consentito portare fuori dall'azienda supporti cartacei od informatici contenenti dati e/o programmi, né utilizzare a tal fine soluzioni cloud o di file sharing.

Poiché i sistemi di trattamento sono strumenti professionali non possono in alcun modo essere utilizzati per scopi personali e qualunque archivio o documento (sia cartaceo che elettronico) estraneo all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in locali, archivi o su supporti di memorizzazione aziendali.
Si precisa esplicitamente che non è consentito prendere visione (anche senza detenerli o scaricarli) od archiviare documenti (informatici o cartacei) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica né materiale pornografico e pedopornografico.
Senza preventiva autorizzazione non è permesso realizzare nuove ed autonome banche dati, né utilizzare le banche dati esistenti per finalità estranee a quelle previste dal Titolare.
Costituisce buona regola la pulizia degli archivi su base almeno semestrale, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati: è, infatti, assolutamente da evitare un'archiviazione ridondante.
E' buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

7 Controlli

Gli strumenti assegnati in uso al Collaboratore (HW, SW, tablet,…) ed i Servizi messi a disposizione degli Utenti sono di natura aziendale ed è precluso ogni utilizzo personale che non sia limitato ed episodico . Anche i dati, i documenti, le informazioni ed i supporti che sono strettamente aziendali ed il loro utilizzo è finalizzato allo svolgimento delle mansioni assegnate, nel rispetto pieno delle finalità dell'Ente, delle istruzioni ricevute, della policy aziendale, dei valori di cui al Codice Etico.
Per far valere o difendere un diritto in sede giudiziaria, per garantire l'operatività, per esigenze di salvaguardia dell'incolumità o per specifici obblighi di Legge, nonché ad accertare eventuali comportamenti illeciti o non in linea con i valori aziendali, Acquedotto Poiana SpA si riserva la possibilità di eseguire audit e vulnerability assesment del sistema informatico, direttamente o avvalendosi di soggetti esterni.
Tali Controlli sono anche finalizzati a valutare e verificare la funzionalità o per garantire la sicurezza del sistema, nonchè ad accertare eventuali comportamenti illeciti o non in linea con i valori aziendali e **non sono preordinati al monitoraggio sull'esecuzione della prestazione lavorativa dei collaboratori**.[6]

In applicazione dei principi di cui all'art. 5 del GDPR, l'organizzazione promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli interessati e, allo scopo, ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.
Acquedotto Poiana SpA precisa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali dei propri collaboratori: in particolare, Acquedotto Poiana SpA non fa utilizzo di sistemi, soluzioni ed accorgimenti atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Incaricati che non rispettino del principio di pertinenza e non eccedenza, né opera registrazioni o verifiche con modalità occulte né analisi indiscriminate.
Le verifiche hanno carattere generale, non sono incentrate sul singolo utente e sono finalizzate alla verifica della funzionalità e dell'operatività del sistema. Qualora nell'ambito di tali verifiche generali si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di file illegali, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un primo avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
Potranno anche essere svolti controlli a campione, dandone preavviso mediante comunicazione a tutto il personale.
Solo in caso di problemi in materia di sicurezza o funzionalità o in caso di abusi singoli o reiterati, potranno essere effettuati controlli individuali ovvero su singoli dispositivi e postazioni, per i quali non verranno inoltrati preventivi avvisi collettivi o individuali. L'analisi potrà interessare anche i file archiviati in copie di backup.

[6] La Corte di Cassazione con la sentenza n. 2722 del 23 febbraio 2012, riconosce il diritto del datore esercitare il potere di verifica «ex post» per accertare eventuali condotte attuate in violazione degli obblighi fondamentali di fedeltà e riservatezza e postasi in contrasto con l'interesse del datore di lavoro. Questi, secondo la Suprema Corte ha il diritto di tutelare il proprio patrimonio, «*costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna presso il pubblico*».

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale avrà luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire le finalità sopra esposte.
Acquedotto Poiana SpA effettuerà controlli non sistematici su tutti gli strumenti messi a disposizione dei collaboratori, compreso l'account di posta elettronica.
E' stato attivato un sistema che blocca i messaggi con allegati potenzialmente pericolosi (ad es. con estensioni .exe, .com, .vbs, .sys, .bin, ecc.). Non viene tenuta traccia dei tentativi di invio dei predetti messaggi da parte del singolo Utente, ma raccolti solo dati aggregati. Il mittente dell'e-mail riceve in automatico una comunicazione dal postmaster che comunica il blocco del messaggio.

L'Ente, effettuerà controlli su tutti gli strumenti messi a disposizione dei collaboratori, compreso l'account di posta elettronica.[7]
Nel caso risulti indispensabile per Acquedotto Poiana SpA procedere all'analisi del contenuto dei messaggi, all'incaricato è accordata la possibilità di individuare un "fiduciario" che avrà accesso ai messaggi di posta elettronica e si preoccuperà di fornire a Acquedotto Poiana SpA le informazioni necessarie allo svolgimento dell'attività lavorativa. A cura di Acquedotto Poiana SpA ogni estrazione verrà redatto apposito verbale e fornita comunicazione all'incaricato.
Durante i controlli, l'Utente ha il diritto di essere presente e di farsi assistere da una persona di fiducia e può richiedere la presenza delle rappresentanze sindacali.
Dell'attività di controllo deve essere redatto un verbale in duplice copia, di cui una viene consegnata al soggetto controllato.
In ossequio alle prescrizioni dell'Autorità Garante italiana di cui al Provvedimento sugli Amministratori di Sistema[8], sono adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Gli "*access log*" comprendono i riferimenti temporali e la descrizione dell'evento, e sono registrati in modo da mantenere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. Vengono conservati per un periodo non inferiore ai sei mesi al fine di consentire la verifica da parte del titolare o dei responsabili del trattamento.
Anche il telefono assegnato in uso è uno strumento di lavoro e, pertanto, Acquedotto Poiana SpA potrà procedere all'analisi dei numeri chiamati, della durata delle conversazioni e potrà inibire chiamate a numerazioni particolari o a categorie di soggetti.

[7] La Corte di Cassazione con la sentenza 19 dicembre 2007, n. 47096, ha stabilito che: «*Non integra il reato di cui all'art. 616 cod. pen. la condotta del superiore gerarchico che prenda cognizione della posta elettronica contenuta nel computer del dipendente, assente dal lavoro, dopo avere a tal fine utilizzato la password in precedenza comunicatagli in conformità al protocollo aziendale*».
8 Si Tratta del Provvedimento "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" (G.U. n. 300 del 24 dicembre 2008) successivamente modificato con provvedimento del 25 giugno 2009 "*Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento*" (G.U. n. 149 del 30 giugno 2009).

8 Validità e revisione della Policy aziendale.

La presente Policy è soggetta a revisione periodica annuale ma anche in occasione di incidenti di sicurezza o nel caso vengano commessi reati presupposto.
Il Delegato ha la responsabilità di sviluppare, revisionare e manutenerne i contenuti della presente policy, assicurandone una piena efficacia in relazione a mutamenti nell'ambiente organizzativo, nella legislazione e di contesto.
Tutti gli utenti possono proporre, quando lo ritengono necessario, integrazioni e correzioni, indirizzando le proposte al Delegato.