MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ex D.Lgs. 231/2001

Trasimeno Servizi Ambientali S.p.A.

Sede legale: Case Sparse, 107, Loc. Soccorso, Magione, Perugia (PG)

PROTOCOLLO 08

Gestione dei sistemi informativi aziendali

Codice documento: PR 08

VERSIONE	DATA EMISSIONE	COMMENTO	APPROVAZIONE
00	25-03-2014	Prima Emissione	Consiglio di Amministrazione
01	14-03-2016	Seconda Emissione	Consiglio di Amministrazione
02	28-08-2018	Terza Emissione	Consiglio di Amministrazione
03	07-01-2021	Quarta Emissione	Consiglio di Amministrazione

INDICE

Funzioni aziendali coinvolte p. 3
Attività sensibili p. 3
Reati astrattamente ipotizzabili p. 3
Principi di comportamento e procedure operative a presidio delle attività sensibili p. 6
Flussi informativi nei confronti dell'Organismo di Vigilanza p. 13
TABELLA RIEPILOGATIVA DEI FLUSSI INFORMATIVI p. 15

Funzioni aziendali coinvolte

La gestione dei sistemi informativi aziendali risulta trasversale a tutti gli ambiti di attività della società, con potenziale coinvolgimento di tutte le funzioni aziendali.

Attività sensibili

Nell'ambito dell'attività di gestione dei sistemi informativi aziendali si individuano le seguenti attività sensibili:

- gestione adempimenti tributari: predisposizione ed invio dati telematici all'anagrafe tributaria e pagamento imposte (Camera di Commercio, Guardia di Finanza, Agenzia delle Entrate);
- acquisto, gestione e utilizzo del sistema informativo e delle licenze software;
- gestione degli incidenti e dei problemi di sicurezza informatica;
- definizione e gestione attività periodica di backup, sistemi antivirus, firewall e protezione della rete, sicurezza fisica server e postazioni;
- verifica degli accessi e tracciabilità delle modifiche ai dati compiute dagli utenti;
- gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio;
- gestione dei contenuti del sito internet della Società.

Reati astrattamente ipotizzabili

Si elencano di seguito i possibili reati configurabili con riferimento alle attività sensibili individuate nella presente area a rischio:

- Art. 615 *ter* c.p. - Accesso abusivo ad un sistema informatico o telematico
- Art. 615 *quater* c.p. - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- Art. 615 *quinquies* c.p. - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- Art. 617 *quater* c.p. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

- Art. 617 *quinquies* c.p. - Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche
- Art. 635 *bis* c.p. - Danneggiamento di informazioni, dati e programmi informatici
- Art. 635 *ter* c.p. - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
- Art. 635 *quater* c.p. - Danneggiamento di sistemi informatici o telematici
- Art. 635 *quinquies* c.p. - Danneggiamento di sistemi informatici o telematici di pubblica utilità
- Art. 171 *bis* l. 633/1941 comma 1 - Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori.

A titolo esemplificativo si potrebbero configurare le seguenti modalità di realizzazione dei reati:

- Il reato di criminalità informatica potrebbe configurarsi nell'interesse o a vantaggio della Società attraverso:

1. l'ottenimento, la riproduzione, la diffusione, la comunicazione o la divulgazione di codici di accesso a sistemi informatici protetti o crittati;
2. l'installazione di apparecchiature atte ad intercettare terze parti e carpire informazioni che possono essere di interesse o vantaggio per la Società;
3. l'installazione di apparecchiature atte al danneggiamento dei sistemi hardware che abbia il fine di procurare un interesse o vantaggio per la Società (ad es. accesso alle copie di backup e distruzione di informazioni che possano essere prova di azioni illecite);
4. la diffusione di programmi capaci di infettare un sistema per manometterne la regolare funzionalità (ad es. il sistema informatico di un competitor);
5. l'accesso abusivo ad un sistema protetto o nel permanervi contro la volontà espressa o tacita in settori (ad es. accesso non autorizzato ai sistemi che realizzano la fatturazione attiva per alterare le informazioni o i programmi al fine di realizzare un profitto illecito per la Società);

6. l'accesso abusivo (non autorizzato) ad un sistema informatico protetto di aziende concorrenti al fine di recepire informazioni nell'interesse o a vantaggio della Società (es. operazioni straordinarie, partecipazione a gare d'appalto, offerta economica presentata, etc.);
7. qualunque condotta strumentale all'ottenimento di password o di qualsivoglia mezzo per entrare in un sistema informatico e far realizzare un profitto ad esempio intercettando una comunicazione tra più parti al fine di veicolare informazioni false o alterate per danneggiare l'immagine di un concorrente o impedendo/interrompendo una comunicazione al fine di arrecare danno economico o di business ad un ente terzo;
8. la falsità di un documento informatico, ovvero di supporto informatico contenente dati o informazioni avente efficacia probatoria o di programma specificamente destinato ad elaborarlo;
9. la trasmissione di falso materiale con un uso illegittimo della firma elettronica altrui, redazione di un falso atto informatico destinato ad essere inserito in un pubblico archivio la cui gestione operativa sia affidata ad una società privata, cancellazione di dati considerati sensibili o rischiosi al fine di controllare o deviare eventuali ispezioni o controlli;
10. l'intercettazione di comunicazioni o informazioni di terze parti che potrebbero portare interesse o vantaggio per la Società (es. operazioni straordinarie, partecipazione a gare d'appalto, offerta economica presentata, etc.);
11. il danneggiamento di programmi informatici di terze parti;
12. il danneggiamento di programmi informatici utilizzati dallo Stato o da altro Ente Pubblico.

- Con riferimento ai reati commessi in violazione del diritto d'autore la Società potrebbe:

1. duplicare abusivamente programmi per elaboratore coperti da licenza al fine di trarne vantaggi economici, oppure utilizzare software non licenziati;
2. importare, distribuire, vendere e detenere a scopo commerciale o imprenditoriale e locazione di software "pirata";
3. utilizzare, per scopi lavorativi, programmi non originali ai fine di risparmiare il costo derivante dalla licenza per l'utilizzo di un software originale;

4. utilizzare qualsiasi mezzo inteso a consentire o facilitare la rimozione arbitraria o l'elusione di protezioni di un software;
5. riprodurre su supporti non contrassegnati SIAE, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca di dati al fine di trarne profitto;
6. inserire nel sito internet della società foto, video o audio protetti da diritti d'autore in assenza di idonea autorizzazione.

Principi di comportamento e procedure operative a presidio delle attività sensibili

- Il Responsabile IT, anche avvalendosi del supporto di un consulente informatico, deve:

1. garantire l'acquisto e l'uso esclusivamente di software autorizzato e certificato;
2. garantire che per installare software diversi da quelli messi a disposizione dalla Società, sia necessario richiedere autorizzazione preventiva all'amministratore di sistema;
3. compilare e mantenere aggiornato un inventario dell'hardware e del software in uso presso la Società;
4. effettuare verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o potenzialmente nocivi;
5. prevedere un piano di *business continuity* ed uno di *disaster recovery* periodicamente aggiornati e testati;
6. prevedere specifici criteri per l'assegnazione e la creazione, modifica e aggiornamento delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (ad es. lunghezza minima della password, regole di complessità, scadenza);
7. far compilare e accettare formalmente a tutti gli assegnatari della dotazione informatica hardware e software una "scheda di presa in carico" dove, previa elencazione di tutta la strumentazione hardware e software fornita, vengono descritte le condizioni d'uso che tutto il personale si impegna a rispettare;
8. prevedere, nella scheda di presa in carico:
    a. l'obbligo di utilizzare il pc per le sole esigenze di servizio;

b. l'obbligo di non cedere, in nessun caso, neppure in via temporanea, l'uso del pc a terzi, né a titolo gratuito né a titolo oneroso, tenendo, in particolare, segreta la password per il collegamento da remoto alla rete aziendale, laddove previsto;

c. il divieto di istallare software non forniti da Trasimeno Servizi Ambientali S.p.A. anche se distribuiti gratuitamente;

d. l'obbligo di conservare e custodire con cura e con la massima diligenza il pc provvedendo alla restituzione dello stesso nello stato attuale, salvo il normale deterioramento, non appena richiesto dalla Società e comunque non oltre il termine massimo da quest'ultima eventualmente fissato, senza possibilità di opporre eccezione alcuna;

e. l'obbligo di comunicare con la massima tempestività l'eventuale smarrimento e/o furto del pc informando in ogni caso la società circa la natura e l'entità dei dati aziendali in esso memorizzati;

f. l'obbligo di comunicare gli eventuali malfunzionamenti del pc alla società mettendo in qualsiasi momento il pc stesso a disposizione della società o di un suo incaricato per ogni operazione di manutenzione e/o riparazione che dovesse essere ritenuta necessaria;

9. gestire la fase della riconsegna del materiale attraverso la compilazione della scheda di "restituzione della dotazione informatica", dove viene fatto espresso divieto di criptare, riservare, rendere comunque inutilizzabili i dati contenuti nel pc oggetto di riconsegna;

10. prevedere, nell'ambito della creazione e della assegnazione dei profili autorizzativi ai dipendenti, che la password di rete inizialmente creata di default dagli amministratori di sistema e assegnata ai dipendenti, sia conservata correttamente e cambiata periodicamente;

11. prevedere il divieto assoluto di cedere e/o comunicare a terzi la password e creare identificativi facilmente decriptabili (es. nome-cognome del dipendente);

12. garantire che le applicazioni tengano traccia delle modifiche ai dati compiute dagli utenti;

13. definire i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;

14. eseguire verifiche periodiche dei profili utente al fine di verificare che siano coerenti con le responsabilità assegnate e coerente con i principi di segregazione dei ruoli;
15. archiviare la documentazione riguardante ogni singola attività allo scopo di garantire la completa tracciabilità della stessa;
16. definire i criteri e le modalità per la gestione dei sistemi hardware che prevedano la compilazione e la manutenzione di un inventario aggiornato dell'hardware in uso presso la Società e che regolamentino le responsabilità e le modalità operative in caso di implementazione e/o manutenzione di hardware;
17. definire i criteri e le modalità per le attività di back up che prevedano, per ogni applicazione hardware, la frequenza dell'attività, le modalità, il numero di copie ed il periodo di conservazione dei dati;
18. definire i criteri e le modalità per la gestione dei sistemi software che prevedano la compilazione e manutenzione di un inventario aggiornato del software in uso presso la società, l'utilizzo di software formalmente autorizzato e certificato e l'effettuazione di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o potenzialmente nocivi;
19. definire le credenziali fisiche di accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT quali, a titolo esemplificativo, codici di accesso, badge, chiavi e la tracciabilità degli stessi;
20. prevedere, per l'accesso a internet, che:
    a. ogni volta che si riceve un'informazione tramite Internet, venga valutata accuratamente la provenienza della stessa;
    b. ogni volta che si devono pubblicare o inviare delle informazioni su internet, è necessario assicurarsi che gli strumenti di sicurezza applicati siano adeguati all'importanza dell'informazione.
21. gli accessi effettuati dagli utenti, in qualsiasi modalità, ai dati, ai sistemi ed alla rete siano oggetto di verifiche periodiche;
22. prevedere, per l'uso della posta elettronica, che:

a. non deve essere considerata sicura la posta elettronica se il destinatario o il mittente sono esterni all'azienda;

b. i dipendenti hanno l'obbligo di usare la dovuta cautela nell'esposizione di concetti che potrebbero essere considerati presa di posizione ufficiale dell'azienda;

23. prevedere ruoli e responsabilità dei soggetti che usano i sistemi informatici e le piattaforme telematiche gestiti da terzi, ivi inclusi ruoli e responsabilità di coloro che operano attraverso strumentazione informatica e telematica;

24. adottare sistemi idonei alla registrazione degli accessi mediante autenticazione informatica ai sistemi informatici e agli archivi elettronici da parte da parte di tutti i dipendenti ivi inclusi gli amministratori di sistema;

25. prevedere limitazioni alla possibilità di scaricare materiale dalla rete internet, adottando sistemi informatici idonei a limitare la possibilità di effettuare download e/o operazioni analoghe non autorizzati;

26. impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;

27. limitare gli accessi alle stanze server unicamente al personale autorizzato;

28. dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;

29. informare gli utilizzatori dei sistemi informatici che i software per l'esercizio delle attività di loro competenza sono protetti dalle leggi sul diritto d'autore ed in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;

30. prevedere nei i contratti che regolano i rapporti con soggetti terzi apposite clausole che impongano:

a. la conformità dei software forniti a leggi e normative ed in particolare alle disposizioni di cui alla L. 633/1941;

b. la manleva per la Società in caso di violazioni commesse dai fornitori del servizio stessi.

➢ Tutti i soggetti in posizione apicale, i Responsabili di Funzione, i dirigenti e i dipendenti assegnatari di strumenti hardware aziendali devono:

1. sottoscrivere la "scheda di presa in carico" al momento della ricezione di strumenti informatici hardware e software;
2. compilare la scheda di "restituzione della dotazione informatica" in fase di riconsegna del materiale informatico;
3. connettere ai sistemi informatici di Trasimeno Servizi Ambientali S.p.A. solo i personal computer e le periferiche fornite dalla Società;
4. richiedere l'autorizzazione dell'amministratore di sistema per l'installazione di software non forniti dalla Società;
5. rispettare gli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano il diritto d'autore;
6. non divulgare, cedere o condividere con personale interno o esterno a Trasimeno Servizi Ambientali S.p.A. le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
7. segnalare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, che potrebbero consentire l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere.

***

I Destinatari del Modello, ed in particolare i soggetti aziendali coinvolti nella presente area a rischio, così come identificati nei precedenti paragrafi, sono tenuti, nello svolgimento delle attività sensibili, a tenere un comportamento corretto e trasparente, in conformità a quanto previsto dalle previsioni di legge vigenti in materia e dal Codice Etico allegato al Modello (vds. par. 3.9 *Norme di comportamento relative ai reati informatici e trattamento illecito di dati*).

In particolare è fatto divieto di:

➢ connettere ai sistemi informatici di Trasimeno Servizi Ambientali S.p.A. personal computer, periferiche, altre apparecchiature o installare software senza preventiva autorizzazione del soggetto aziendale responsabile individuato;

- modificare la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;
- acquisire, possedere o utilizzare strumenti software e/o hardware – se non per casi debitamente autorizzati ovvero in ipotesi in cui tali software e/o hardware siano utilizzati per il monitoraggio della sicurezza dei sistemi informativi aziendali – che potrebbero essere adoperati abusivamente per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le Credenziali, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);
- ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate da Trasimeno Servizi Ambientali S.p.A.;
- divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- accedere abusivamente ad un sistema informatico altrui – ovvero nella disponibilità di altri Dipendenti o terzi – nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- comunicare a persone non autorizzate, interne o esterne a Trasimeno Servizi Ambientali S.p.A., i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
- mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti Virus o altri programmi in grado di danneggiare o intercettare dati;
- inviare attraverso un sistema informatico aziendale qualsiasi informazione o dato, previa alterazione o falsificazione dei medesimi;

- installare prodotti software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano il diritto d'autore;
- duplicare, distribuire, vendere o detenere a scopo commerciale/imprenditoriale software;
- utilizzare programmi non originali;
- utilizzare mezzi intesi a consentire o facilitare la rimozione arbitraria o l'elusione di protezioni di un software;
- riprodurre su supporti non contrassegnati SIAE, trasferire su altro supporto, distribuzione, comunicare, presentare o dimostrare in pubblico il contenuto di una banca di dati;
- acquisire e/o utilizzare prodotti tutelati da diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;
- porre in essere comportamenti idonei a violare le norme di legge e le procedure aziendali interne poste a tutela dello sfruttamento dei diritti d'autore.

È fatto obbligo di:

- custodire e proteggere le informazioni e i documenti riservati in maniera adeguata e continua;
- informare ogni collaboratore dell'obbligo della riservatezza sulle informazioni non pubbliche di cui è venuto a conoscenza per ragioni d'ufficio;
- comunicare le informazioni riservate solo a coloro che devono venirne a conoscenza per svolgere il compito loro affidato;
- gestire il trattamento di informazioni personali nel pieno rispetto della legge sulla Tutela dei dati personali, seguendo scrupolosamente le istruzioni rilasciate dalle Società nella lettera di incarico;
- utilizzare solamente i dati strettamente necessari per l'esecuzione dei compiti loro affidati e per le finalità proprie della loro funzione;
- garantire che le informazioni non siano duplicate o diffuse;
- custodire gli archivi secondo le misure di sicurezza previste dalla Società, volte a limitare l'accesso ai dati solo a coloro che ne sono espressamente autorizzati;
- osservare il dovere di riservatezza anche dopo la cessazione dal servizio;

- consultare i soli documenti cui sono autorizzati ad accedere, facendone uso conforme alle proprie mansioni e consentendone l'accesso solo a coloro che ne abbiano titolo ed in conformità alle prescrizioni impartite;
- prevenire l'eventuale dispersione di dati osservando le misure di sicurezza impartite, custodendo con ordine e cura gli atti affidati ed evitando di effettuarne inutili copie.

***

Tutta la documentazione prodotta o acquisita nell'ambito delle attività disciplinate nel presente protocollo è conservata a cura dei Responsabili delle Funzioni aziendali coinvolti, che dovranno documentare, se del caso, l'attribuzione ad altri soggetti aziendali della responsabilità della conservazione della documentazione in questione.

La stessa è, inoltre, messa a disposizione, su richiesta, solo ed esclusivamente ai soggetti autorizzati sulla base delle procedure aziendali e dell'organizzazione interna.

I documenti prodotti nell'ambito delle attività descritte nel presente protocollo devono essere conservati per un periodo di dieci anni.

Flussi informativi nei confronti dell'Organismo di Vigilanza

- Il Responsabile IT deve redigere apposito report da inviare all'OdV con periodicità annuale avente ad oggetto gli aspetti significativi afferenti le diverse attività di propria competenza in particolare per quanto attiene:

1. alle attività di salvaguardia delle attrezzature hardware e software presenti in azienda,
2. ai controlli e le verifiche periodiche della efficienza del sistema informatico,
3. all'aggiornamento dell'inventario dei software in uso presso la Società e delle relative licenze nonché dell'elenco degli strumenti hardware assegnati ai dipendenti (con allegate le "schede di presa in carico" sottoscritte al momento della ricezione),
4. alle autorizzazioni concesse ai fini di abilitare gli accessi degli utenti alle funzionalità dei sistemi informativi,
5. ad eventuali incidenti IT verificatosi, e i relativi processi di risposta attivati.

- Il Responsabile IT deve in ogni caso comunicare immediatamente all'OdV ogni manomissione o altra significativa anomalia riscontrate nelle procedure di salvaguardia, accesso al sistema e ai dati aziendali ed elaborazione dei medesimi e nell'utilizzo del sistema informatico aziendale, in particolare relativamente alle attività di elaborazione e trasmissione di dati contabili, fiscali e gestionali.

Adeguata comunicazione deve essere trasmessa da parte del Responsabile IT anche qualora non vi sia nulla da segnalare nel periodo di riferimento.

Si rimanda al PROTOCOLLO 11 - *Segnalazioni e flussi informativi periodici all'OdV*- per maggiori dettagli circa l'oggetto e le modalità delle comunicazioni all'OdV.

PROTOCOLLO 08 – GESTIONE DEI SISTEMI INFORMATIVI AZIENDALI			
FLUSSI INFORMATIVI PERIODICI			
Area a rischio	**Contenuto**	**Periodicità**	**Funzione Segnalante**
N. 1 Gestione dei sistemi informativi aziendali	*Report* aventi ad oggetto: – Attività di salvaguardia delle attrezzature Hardware e software presenti in azienda; – Controlli e verifiche periodiche dell'efficienza del sistema informatico; – Aggiornamento dell'inventario dei software in uso presso la Società e delle relative licenze, nonché l'elenco degli strumenti hardware assegnati ai dipendenti; – Autorizzazioni concesse ai fini di abilitare gli accessi degli utenti alle funzionalità dei sistemi informativi; – Eventuali incidenti verificatosi, e i relativi processi di risposta attivati.	Annuale	– *Responsabile IT*