UN MONDO DI SERVIZI SOCIETA' A RESPONSABILITA' LIMITATA SEMPLIFICATA
VIA MICHELE PIRONTI 45 - 00165 ROMA (RM)
B000584193 del 12-10-2017

POLICY

CYBER SECURITY AZIENDALE

Data di emissione: 19.06.2025

Documento composto da 8 pagine

Rev	Data	Descrizione
4	08.01.2025	Aggiornamento periodico
3	08.01.2024	Aggiornamento periodico
2	01.09.2023	Aggiornamento periodico
1	01.09.2022	Aggiornamento periodico
0	15.09.2021	Prima stesura

Steso e verificato da *Addetto Revisione Interna*	ing. Francesco Netti	

	Cognome	Nome	Firma
Approvato da *Delegati Assicurativi*	GIUNCATO	VITTORIO	

Sommario

1. Scopo e campo di applicazione

La presente procedura descrive le modalità operative, messe in atto dalla Direzione, per ottenere un'adeguata gestione dei sistemi informatici e volte a prevenire i delitti informatici e il trattamento illecito dei dati. Quanto qui prescritto deve essere applicato a tutto il personale che opera all'interno dell'Organizzazione.

2. Riferimenti normativi

RIFerimento	anno	descrizione
Regolamento UE 679	2016	Disposizioni in materia di trattamento dei dati personali e di privacy
Decreto legislativo 231	2001	Disposizioni attuative volte a prevenire i delitti informatici e il trattamento illecito dei dati. Art. 24 bis del D.lgs 231/2001 aggiunto dall'art. 7 della legge n.48 del 2008.

3. Identificazione dei reati

Ai sensi dell'art. 24 bis del D.lgs. 231/2001, aggiunto dalla Legge n. 48 del 2008, si individuano nella successiva tabella, le attività che potrebbero dar luogo a dei reati considerati di responsabilità dell'Agenzia.

Reati Analizzati	Applicabile	Non Applicabile	Attività sensibili	Istruzione impostata

Art. 615 ter c.p. Accesso abusivo ad un sistema informatico o telematico	**X**		Accesso accidentale o non autorizzato	Istruzione 4.3
Art. 615 quarter c.p. Detenzione e diffusione abusivi di codici di accesso a sistemi informatici o telematici	**X**		Divulgazione non autorizzata di dati	Istruzione 4.3
Art. 615 quinquies c.p. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	**X**		Sistemi informatici non protetti	Istruzione 4.2
Art. 617 quater c.p. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematica		**X**	-	-
Art. 617 quater c.p. Installazione si apparecchiature atte a intercettare, impedire od interrompere comunicazioni informatiche o telematiche		**X**	-	-
Art. 635 bis c.p. Danneggiamento di informazioni dati e programmi informatici	**X**		Distruzione, perdita o modifica dei dati	Istruzione 4.1
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		**X**		
Art. 635 quarter c.p. Danneggiamento di sistemi informatici o telematici	**X**		Accesso accidentale o non autorizzato alla rete e agli applicativi	Istruzione 4.1
Art. 635 quinquies c.p. Danneggiamento di sistemi informatici telematici di pubblica utilità	**X**		Accesso accidentale o non autorizzato alla rete e agli applicativi	Istruzione 4.1
Art. 640 quinquies c.p. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica		**X**		
Art. 491 bis c.p. Falsità in documenti informatici	**X**		Inserimento dati banca dati agenziale	Gestione contatto cliente

4. Istruzioni operative

4.1 Istruzioni utilizzo della rete

4.1.1 Oggetto e ambito di applicazione

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

4.1.2 Principi generali – diritti e responsabilità

L'agenzia promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità. Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.
Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.
Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.
Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.
Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

4.1.3Abusi e attività vietate

E' vietato ogni tipo di abuso. In particolare, è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri, trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;

- utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile.

4.1.3 Attività consentite

E' consentito all'amministratore di sistema:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei clienti e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura descritta nell'informativa privacy dedicata;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

4.1.4 Soggetti e modalità di accesso alla rete e agli applicativi

Hanno diritto ad accedere alla rete tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.
L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.
L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.
Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili, l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.
L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.
Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.
L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente

regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.
L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.
L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.
Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dal custode delle password e rispettare le norme concordate.
In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti interni.

4.2 Istruzioni di comportamento per minimizzare i rischi da virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC , XLS;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di “scaricare“ dalla rete internet ogni sorta di file, eseguibile e non. La decisione di “scaricare” può essere presa solo dall'amministratore di sistema;
- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su “chiedi conferma” (il browser avvisa quando uno script cerca di eseguire qualche azione);
- attivare la protezione massima per gli utenti del programma di posta Outlook Express (o ad altri gestori di posta elettronica) al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta,(in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
- non attivare le condivisioni dell'HD in scrittura.
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;

- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore e/o il tecnico esterno incarico dell'assistenza procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

- formattare l'Hard Disk, definire le partizioni e reinstallate il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
- installare il software antivirus, verificare e installare immediatamente gli eventuali ultimi aggiornamenti;
- reinstallare i programmi applicativi a partire dai supporti originali;
- effettuare il RESTORE dei soli dati a partire da una copia di backup recente. NESSUNPROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;
- effettuare una scansione per rilevare la presenza di virus nelle copie dei dati; ricordare all'utente di prestate particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

4.3 Istruzioni per la gestione delle password

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato User-id) e password personale.

User-id e password iniziali sono assegnati dal custode delle password.

User-id e password sono strettamente personali e non possono essere riassegnati ad altri utenti. La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore.

Ogni tre mesi il sistema richiede automaticamente il cambio delle password di accesso; ciascun incaricato provvede a sostituire la propria password e a comunicare la variazione effettuata al custode delle password.

Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.

In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte. Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili: le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo; per la definizione/gestione della password devono essere rispettate le seguenti regole:

- la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
- deve contenere almeno un carattere alfabetico ed uno numerico;
- non deve contenere più di due caratteri identici consecutivi;
- non deve contenere la user-id come parte della password;
- al primo accesso la password ottenuta dal custode delle password deve essere cambiata;
- la nuova password non deve essere simile alla password precedente;
- la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;

- la password termina dopo sei mesi di inattività;
- la password è segreta e non deve essere comunicata ad altri;
- la password va custodita con diligenza e riservatezza;

- l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia.

4.4 Regole sicurezza informatica

Compiti assegnati all'Amministratore di Sistema:

■ Inventario hardware e software;

è necessario che l'amministratore di sistema si dedichi alla gestione e alla manutenzione di impianti di elaborazioni con cui vengono effettuati trattamento dati personali, compresi i sistemi di gestione delle base dei dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

Viene redatto *l'inventario dei dispositivi hardware e software*, che dev'essere aggiornato periodicamente. Devono essere indicati i dispositivi fisici (hardware) e i programmi (software), con le rispettive licenze, e tutti i sistemi, i servizi e le applicazioni informatiche utilizzate all'interno dell'azienda. Per quanto riguarda le applicazioni, i sistemi informatici e i programmi in uso forniti da terze parti (spazi web, servizi cloud, social network e posta elettronica) devono essere ridotti a quelli strettamente necessari per lo svolgimento dell'attività dell'impresa. È necessario aggiornare l'inventario quando ci sono nuovi dispositivi e software installati o collegati alla rete. Per i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine e la funzione del sistema. L'inventario deve includere dispostivi come telefoni cellulari, tablet e laptot e altri dispositivi elettronici portatili che memorizzano o elaborano dati.

■ Gestione della configurazione dei PC;

La configurazione è necessaria affinché i programmi installati nel PC possano funzionare correttamente. L'amministratore compila la scheda controllo sicurezza informatica. Devono essere individuati il numero dei PC, il sistema operativo, l'indicazione dell'aggiornamento periodico e l'amministratore. Inoltre, dev'essere presente lo screen saver, back up periodico e l'antivirus.

■ Analisi della vulnerabilità;

La vulnerabilità informatica del software è la segnalazione di una falla in un computer.

è necessario analizzare se i dispositivi sono protetti da virus, malware e tentativi di intrusione. I PC devono essere dotati di Antivirus. È vietato installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete e utilizzare la rete per scopi connessi all'attività designata. Abusi e attività vietate sono sopra descritte nelle istruzioni.

5 Verifiche periodiche

Il presente registro viene modificato al mutare degli elementi contenuti tenendo conto delle modalità e le tipologie del trattamento con cadenza almeno biennale.

È presente un report annuale (Allegato 1 Policy Cyber Security Aziendale) compilato dall'amministratore di sistema sul grado di applicazione delle misure minime di sicurezza. I requisiti di un sistema di sicurezza informatico sono volti all'integrità, alla riservatezza e alla disponibilità dei dati memorizzati tramite strumenti elettronici.