REGOLAMENTO SERVIZI INFORMATIVI

DI

ALES SPA

Il presente regolamento, è realizzato sulla base e seguendo le linee guida contenute nella circolare AGID del 18/04/2017 (Disposizioni in materia di sicurezza informatica), nel Regolamento UE 2016/679 del 27/04/2016 (GDPR - regolamento generale sulla protezione dei dati) e nella direttiva della Presidenza Consiglio Ministri n. 02/09 (utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro), ha per oggetto i criteri e le modalità di utilizzo del servizio di informativi e, più in particolare, delle dotazioni IT di Ales da parte dei propri dipendenti, dirigenti e dei collaboratori che, a vario titolo, svolgono un'attività per conto di Ales accedendo all'infrastruttura informativa (di seguito, "utenti").

Introduzione

La crescente diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai PC, espone Ales spa e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità conseguenti alla violazione di specifiche disposizioni normative creando problemi alla sicurezza e alla immagine dell'azienda.

Considerato inoltre che Ales, nell'ottica di uno svolgimento più agevole della propria attività, mette a disposizione dei propri collaboratori che ne necessitano per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, tablets, telefoni cellulari, smartphone, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità e ai doveri che ciascun collaboratore deve osservare nell'utilizzo di detta strumentazione.

Le risorse ICT, messe a disposizione da Ales, oggetto di tutela da parte del presente documento, sono:

- − il patrimonio informativo detenuto da Ales, in formato elettronico;
- − i servizi informatici erogati da Ales;
- − le postazioni di lavoro "fisse" (PC desktop e simili) e "mobili" (PC portatili e simili);
- − i dispositivi cellulari (smartphone);
- − i software di comunicazione (tipo "messenger" e simili);
- − i server, le apparecchiature e tutto il materiale hardware in generale

Finalità del presente documento

Il presente documento si prefigge di tutelare le risorse ICT di Ales e di fornire indicazioni agli Utenti circa il corretto ed appropriato uso delle stesse. Ales, in particolare, intende perseguire i seguenti obiettivi:

- ridurre i rischi relativi alle minacce di sicurezza informatica, preservando la disponibilità, integrità e confidenzialità dei dati;
- continuità dei servizi erogati; garantire il rispetto della normativa in materia.

Contesto Normativo di riferimento

1. Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE", che sarà direttamente applicabile in tutti gli Stati dell'Unione europea a partire dal 25 maggio 2018 (d'ora in poi "GDPR");
2. D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" (d'ora in poi "Codice");
   Provvedimenti del Garante per la protezione dei dati personali in materia di "misure di sicurezza", in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008).
3. Garante della privacy "Linee guida per posta elettronica e internet" del 01.03.2007 Direttiva n. 2/2009 del Dipartimento Funzione Pubblica ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro".

Ambito di applicazione del presente documento

Il presente documento si applica ai soggetti di seguito indicati e, per brevità, definiti "Utenti":

a) Direttori e dipendenti, a qualsiasi titolo inseriti nell'organizzazione aziendale, senza distinzione di ruolo e/o livello;

b) consulenti e collaboratori dell'Azienda, a prescindere dal rapporto contrattuale intrattenuto con la stessa;

c) dipendenti e collaboratori di società che hanno un contratto in essere con l'Azienda e che utilizzano risorse ICT della stessa;

d) ospiti dell'Azienda, per l'eventuale uso delle risorse ICT della stessa;

e) Enti e Agenzie attestati alla rete Intranet, per quanto applicabile.

Le norme si rivolgono a differenti categorie di soggetti essendo destinate a disciplinare sia il comportamento di Utenti "meri utilizzatori" (fruitori di PC desktop, smartphone, PC portatili, ecc.), sia il comportamento di Utenti che svolgono mansioni tecniche (Amministratori di Sistema, Amministratori di Rete, gestori di banche dati, gestori di servizi, ecc.). Ciascun Utente, in base al proprio profilo "base" o "evoluto", dovrà attuare le norme che sono allo stesso indirizzate nel caso di dubbi di applicazione delle stesse, rivolgersi alla divisione IT.

Regole per il corretto uso delle risorse ICT

Premessa

Le regole sono declinate su tre versanti: organizzativo, tecnologico-procedurale e comportamentale. Tutti gli interventi sono finalizzati a garantire la confidenzialità, l'integrità e la disponibilità delle informazioni di Ales.

In particolare:

- La confidenzialità o riservatezza riguarda la conoscibilità e fruibilità delle informazioni ai soli soggetti autorizzati;
- L'integrità è relativa alla completezza ed inalterabilità delle informazioni;
- La disponibilità concerne l'accessibilità ed usabilità delle informazioni nel tempo da parte dei soggetti autorizzati.

Soluzioni organizzative

Ciascun Responsabile del trattamento dei dati personali designa un Referente Privacy all'interno della propria struttura e segnala il nominativo al DPO (Data Protection Officier).

Gestione degli incidenti e databreach

Ogni incidente (ad es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete) deve essere segnalato dall'Utente in modo tempestivo alla divisione IT e al Dpo, che raccoglierà le segnalazioni e avvierà il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative.

Nel caso l'incidente di una certa gravità riguardi il patrimonio Informativo e di conoscenza detenuto dall'Azienda oppure le applicazioni informatiche, il DPO e Amministratore di sistema informeranno il Titolare del Trattamento. Per gli incidenti che possono determinare una violazione dei dati personali, cioè la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (cd. "databreach") l'art. 33 del GDPR prevede che in caso di violazione dei dati personali, "il titolare del trattamento notifica la violazione all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del successivo art. 34 disciplina il caso in cui la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche: in tal caso è necessario comunicare la violazione all'interessato senza ingiustificato ritardo, a meno che non si verifichino le circostanze indicate nel paragrafo 3 dell'articolo:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Per ottemperare agli obblighi imposti dalla norma ogni Utente, segnala anche al proprio Direttore le violazioni o gli incidenti informatici che ha rilevato e che possono avere un impatto significativo sui dati personali. Il Direttore/Responsabile dei dati avvisa il DPO e Responsabile dei servizi informativi (mail: privacy@ales-spa.com) e, unitamente, procedono alle comunicazioni del l'avvenuto incidente di databreach e all'avvio dell'istruttoria per la comunicazione all'interessato.

Sicurezza dei server

I gestori di server devono configurare i server medesimi conformemente agli standard di sicurezza e/o best practices (ad es. abilitare soltanto i servizi strettamente necessari, applicare sistematicamente le "pacth", ecc.) emessi da Enti ed Organizzazioni internazionali (ad es. International Standard Organization - ISO, National Institute of Standards and Technology - NIST, Sans Intitute, ecc.) Laddove le strutture si avvalgano di propri fornitori dovranno prevedere nei contratti di appalto l'obbligo di rispettare i predetti standard di sicurezza e, inoltre, dovranno prevedere clausole di "responsabilità esterna" e di "amministrazione dei sistemi", in attuazione del Provvedimento Generale del Garante dei dati personali del 27.11.2008 (in materia di Amministratori di Sistema), come modificato con successivo Provvedimento Generale del 25.06.2009.

Sicurezza delle applicazioni

Le strutture di business che dovessero ricevere la richiesta di sviluppo applicazioni informatiche devono informare la divisione IT di Ales che procederà a richiedere di rispettare l'approccio della "privacy by design", incorporando sia i principi e le misure a tutela della privacy nell'intero ciclo di vita delle applicazioni che, per le applicazioni web based, le best practices emesse dall'Organizzazione internazionale Open Web Application Security Project (OWASP); Il GDPR, stabilisce che: " in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati

fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici."

Utilizzo di dispositivi cellulari e computer portatili

L'utilizzo di dispositivi cellulari e computer portatili, all'esterno dei locali dell'Azienda, deve essere oggetto di particolare cura ed attenzione da parte degli Utenti perché tale utilizzo rappresenta una fonte di rischi particolarmente rilevante in termini di sicurezza, sia delle risorse in sé sia dei dati nelle stesse contenuti. Tali dispositivi, infatti, possono essere soggetti a smarrimento, furti, distruzione o compromissione dei dati, tentativi di frode e/o accesso non autorizzato ovvero essere "infettati" da virus o codice malevole. Per altro un'eventuale contaminazione da virus informatici potrebbe diffondersi e ripercuotersi all'intera rete informatica di Ales, una volta che tali dispositivi siano collegati direttamente alla rete interna.

E' necessario, pertanto, adottare ulteriori norme comportamentali nonché specifiche procedure, di seguito descritte, che gli Utenti sono chiamati ad applicare in modo scrupoloso:

- cifrare i dati (laddove possibile e previa analisi dei rischi/costi-benefici);
- fare periodicamente delle copie di back-up dei dati e verificarle regolarmente;
- attestarsi, con frequenza almeno settimanale, alla rete intranet dell'Azienda per scaricare gli aggiornamenti (patch, hot fix ed elenchi dei virus);
- mantenere abilitato l'antivirus;
- non disabilitare le impostazioni di sicurezza originariamente impostate da Ales;
- evitare di accedere e navigare in siti web "pericolosi" per la sicurezza informatica, a prescindere dal fatto che ciò avvenga al di fuori dell'orario di lavoro;
- non mantenere abilitati protocolli insicuri di comunicazione, come ad es. il Bluetooth, oltre il tempo strettamente necessario.
- Divieto di utilizzo di messaggistica (whatsapp, telegram etc) che non siano aziendali

Modifiche delle risorse ICT

Per quanto riguarda le modifiche si devono distinguere:

a) modifiche hardware degli strumenti di Ales: gli Utenti non devono intervenire sui dispositivi, togliendo, sostituendo od installando componenti hardware (ad esempio masterizzatori CDROM/DVD, schede LAN, ecc.) senza autorizzazione della Divisione IT.

b) modifiche software: gli Utenti non devono modificare i parametri di configurazione dei dispositivi assegnati, salvo che ciò avvenga su precisa autorizzazione della divisione IT. Sono fatte salve le personalizzazioni a livello Utente che non abbiano conseguenze negative sulla funzionalità dei dispositivi stessi. Gli Utenti, inoltre, non devono alterare la configurazione originaria del dispositivo ricevuto in uso (ad es. disinstallando, eseguendo o installando applicazioni che interferiscano sul funzionamento del dispositivo medesimo) senza autorizzazione della divisione IT.

Smarrimento e furto delle risorse ICT

Nei casi di smarrimento, furto accertato o grave manomissione dei dispositivi assegnati o del loro contenuto, gli Utenti devono segnalare tempestivamente l'accaduto ai soggetti di seguito indicati:

Autorità Giudiziaria (sporgendo denuncia);

Ufficio acquisti di Ales – mail: richiesteacquisti@ales-spa.com ;

Direttore della propria Struttura di appartenenza;

Responsabile servizi informativi mediante comunicazione formale

Il patrimonio informativo e di conoscenza detenuto da Ales si suddivide in due macroaree:

-dati personali;
- dati (riservati o non riservati) diversi da quelli personali.

Le due fattispecie necessitano di trattamenti peculiari, fatte salve le più generali cautele e misure di sicurezza descritte a proposito dei dispositivi come più sopra indicato.

Dati personali

In questo paragrafo si vuole porre l'attenzione sugli aspetti di sicurezza relativi al trattamento di dati personali.

Ai fini della corretta applicazione delle indicazioni che seguono, si ritiene utile riportare di seguito la classificazione dei dati personali fatta dal legislatore.

a) I dati personali devono essere trattati e protetti secondo quanto previsto dal GDPR e dal Codice.

b) i dati personali, oggetto di trattamento, devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita,

Ai sensi dell'Art. 4 del GDPR, è un "dato personale", qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

c) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

4. d) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
5. e) Specifiche misure di sicurezza (c.d. "misure minime" di sicurezza) sono prescritte dagli artt. 33-36 e Allegato B del Codice e, ai fini di questo documento, sono destinate ad Utenti diversi (gestore del servizio/sistema,

direttore/responsabile del trattamento, utente/incaricato del trattamento). Ad es. spettano al gestore del servizio gli obblighi in tema di autenticazione informatica; al Responsabile del trattamento la nomina degli Incaricati e l'aggiornamento periodico dell'ambito di trattamento consentito; agli Incaricati del trattamento attenersi alle istruzioni ricevute con la nomina e adottare le necessarie cautele per la segretezza della password.

f) All'atto della dismissione di supporti che contengano dati personali è necessario distruggere o rendere inutilizzabili (cancellandone il contenuto) i supporti medesimi, secondo quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008 sui "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali".

Dati particolari/sensibili e giudiziari/ relativi a condanne penali e reati

Tutti gli Utenti devono porre particolare attenzione nei trattamenti dei dati personali particolari/sensibili e giudiziari/ relativi a condanne penali e reati (definiti all'art. 9 del GDPR ed all'art. 4 del Codice) in relazione alla confidenzialità dei dati. Sono indicati alcuni comportamenti o regole minime da rispettare: cifrare i dati memorizzati sui file/database o in fase di trasferimento; proteggere i canali di trasmissione; evitare l'invio con la posta elettronica di dati sensibili e giudiziari; recuperare tempestivamente i documenti stampati o ricevuti via fax che contengano dati sensibili o giudiziari per sottrarli alla vista di chi non è autorizzato; separare logicamente i dati "comuni" da quelli sensibili/giudiziari nei database, ecc.

Dati diversi da quelli personali

Fatto salvo il requisito dell'Integrità, i dati diversi da quelli personali (definiti al precedente sono classificati in base al livello di Confidenzialità (Confidentiality) come segue: dati riservati e dati non riservati.

Dati riservati

Appartengono a questa categoria i dati a cui siano collegati interessi giuridicamente rilevanti (come ad es. la proprietà individuale, il diritto d'autore e i segreti commerciali). La gestione, trasmissione e condivisione dei dati riservati deve essere sottoposta a particolari cautele e misure, stabilite dal soggetto responsabile, al fine di preservare la confidenzialità dei dati medesimi. L'eventuale manutenzione, effettuata

da partner privati, sui sistemi ed apparati che ospitano dati riservati deve essere disciplinata, a livello contrattuale, prevedendo specifici obblighi di riservatezza a carico dei partner privati.

Dati non riservati

Appartengono a questa categoria: i dati il cui accesso e/o utilizzo non ha restrizioni (ad es. gli "Open Data", i dati oggetto di "accesso civico", ecc.)

Per i dati non riservati, il responsabile stabilisce le forme e modalità attraverso cui rendere disponibili e/o liberamente accessibili i dati nel rispetto della normativa vigente.

Modalità di accesso alla rete ed utilizzo delle postazioni informatiche

Per accedere ai servizi informatici da una postazione di lavoro l'utente deve obbligatoriamente utilizzare un id identificativo (nome utente) e una parola chiave segreta (password complessa). Superato il sistema di autenticazione, l'utente è collegato alla rete protetta di Ales spa e ad internet. Ciascuna postazione di lavoro è assegnata nominalmente ad un utente dalla funzione IT di Ales. In caso di necessità operativa è sempre possibile, da parte di ciascun utente, accedere alla rete tramite un'altra postazione utilizzando le proprie credenziali. L'utente ha l'obbligo di non comunicare le proprie credenziali di accesso a nessuno e deve essere consapevole del fatto che permettere l'accesso a terzi con le proprie credenziali lo espone a responsabilità civile e penale per eventuali utilizzi illeciti.

Preso atto di tale conseguenza, l'utente si impegna a:

- mantenere riservata la password;
- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione ad altri;
- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema; con le proprie credenziali; nel caso l'utente abbia necessità di allontanarsi è obbligato a bloccare la propria postazione di lavoro utilizzando la sequenza di tasti 'ctrl-alt-canc' e il tasto 'blocca'.
- E' evidente che lasciare un PC incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso;
- non utilizzare le postazioni lasciate incustodite e sbloccate dai colleghi.

Le attività di gestione e manutenzione degli strumenti It di Ales spa fanno capo alla Divisione IT e non è consentito agli utenti di intervenire personalmente sulle apparecchiature informatiche.

In particolare:

- è tassativamente proibito installare programmi software non autorizzati, anche se legali, e/o modificare la configurazione hardware della propria postazione di lavoro. Qualora venissero trovati programmi non autorizzati sulle stazioni di lavoro questi verranno disinstallati dal personale tecnico addetto alla manutenzione dei Personal Computer;
- le unità di rete (Fileserver:, C:,...) sono aree di condivisione di informazioni relative all'attività lavorativa e non possono essere utilizzate per il salvataggio di file non istituzionali. Su queste unità vengono svolte attività di gestione e backup da parte dell'divisione IT che potrà procedere alla rimozione senza obbligo di comunicazione all'utente di files o applicazioni ritenute pericolosi per la sicurezza del sistema o non inerenti all'attività lavorativa;
- gli utenti devono rispettare diritti d'autore, copyright e licenze d'uso di software, materiali audiovisivi, documenti ed ogni altra informazione digitale protetta a norma di legge;
- è proibita l'attivazione di hardware (es. PC portatili) non di proprietà dell'ente sulla rete dati e wifi di Ales.

Modalità di utilizzo di postazioni 'mobili'

Ales consegna in dotazione ad alcuni dipendenti notebook. Le regole di utilizzo di queste apparecchiature sono le stesse dei PC collegati alla rete locale anche se i servizi disponibili e la loro modalità di erogazione potrebbe differenziarsi dalle postazioni 'fisse'. I notebook che rimangono sconnessi a lungo dalla rete non ricevono gli aggiornamenti automatici e possono avere quindi un livello di protezione non allineato con gli standard di Ales. E' quindi a carico dell'utilizzatore garantire la funzionalità e l'aggiornamento del sistema.

Posta Elettronica -Mail-Pec

Il servizio di posta elettronica è disponibile per ogni dipendente in forma centralizzata.

Per i nuovi dipendenti assunti la richiesta di creazione di nuova casella mail deve provenire dagli Uffici del Personale di Ales tramite mail all'indirizzo it@ales-spa.com.

L'indirizzo di posta elettronica è composto da iniziale.nome.cognome@ales-spa.com (in caso di omonimia viene aggiunto una lettera del nome). Sono inoltre messe a disposizione degli uffici indirizzi di posta elettronica non nominali, condivisi fra più utenti, che possono essere richiesti soltanto da Dirigenti inviando una comunicazione via mail a it@ales-spa.com .

Nell'utilizzo della posta devono essere adottate le seguenti misure di tipo organizzativo-tecnologico:

- l'assegnazione della casella di posta avviene unicamente per ragioni di servizio;
- le caselle nominali sono da ritenersi personali e accessibili esclusivamente da parte dell'utente proprietario attraverso l'inserimento di una password; la password deve essere mantenuta riservata e non deve essere comunicata.
- La password della propria casella mail verrà richiesta di cambiare ogni 90 gg. Il cambio è obbligatorio su tutti i sistemi informatici assegnati. L'utente, utilizzando le apposite funzioni di delega fornite dal sistema di posta può comunque concedere, in caso di necessità e per ragioni di servizio, l'accesso e l'utilizzo della propria casella ad altri colleghi. I diritti di utilizzo delle caselle di posta non nominali sono stabiliti dalla divisione IT di Ales.
- per evitare di far inserire il dominio @ales-spa.com in blacklist di gestori di posta esterni, bloccando di fatto tutte le mail in uscita dell'ente, si è posto a 500 il limite massimo di mail inviabili in un'ora a indirizzi di posta esterni all'ente;
- l'invio di e-mail con allegati a mittenti multipli deve essere limitata onde evitare sovraccarico sul server e sulle linee esterne. La dimensione massima degli allegati accettati dal sistema di posta è 8Mb;
- è a disposizione di ciascun lavoratore una apposita funzionalità di sistema che consente di inviare automaticamente, in caso di assenze programmate, messaggi di risposta personalizzabili segnalando eventualmente l'indirizzo della persona da contattare;
- le caselle di posta elettronica devono essere utilizzate cancellando sistematicamente i messaggi non necessari per ragioni di servizio, quelli con allegati ingombranti che vanno cancellati. Il limite massimo di ogni casella mail

è 5GB superata la soglia la mail verrà bloccata. Unico modo per lo sblocco è la cancellazione dei messaggi.

In ogni caso è tassativamente vietato:

- utilizzare tecniche di “mail spamming” cioè di invio massiccio di comunicazioni a liste di distribuzione esterne o di azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare 'catene di S. Antonio', appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), giochi, scherzi, barzellette, messaggi inerenti a virus, etc...;
- utilizzare la casella personale per l'iscrizione a dibattiti, forum o mailing-list se non inerenti alla propria attività lavorativa;
- utilizzare il servizio di posta elettronica per trasmettere pubblicità personale o commerciale.

Utilizzo di Internet

Tutti gli utenti a cui è stato assegnato un ID Utente possono collegarsi alla rete internet il cui utilizzo è consentito unicamente per ragioni di servizio. L'utente è direttamente responsabile dell'uso di internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera. L’utilizzo imprudente di alcuni servizi della rete Internet può essere fonte di particolari minacce alla sicurezza del sistema (esempio virus informatici) e all’immagine di Ales.

Nell'utilizzo di internet è vietato:

- L’utilizzo e la consultazione di social network sono permessi esclusivamente per finalità istituzionali
- lo scarico (upload e/o download) di files e/o programmi software, se non esplicitamente autorizzati;
- la partecipazione a Forum non autorizzati, l’utilizzo di chat line, di bacheche elettroniche e la registrazione in guestbooks anche utilizzando pseudonimi (o nicknames) e, più in generale, qualunque utilizzo di questi servizi Internet se non strettamente connessi all'attività lavorativa;

- l'utilizzo del collegamento ad internet per attività in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- l'utilizzo di sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting o similari, così come connettersi a siti che trasmettono programmi in streaming (come radio o TV via WEB) senza espressa autorizzazione.
- Tuttavia l'utilizzo di internet per svolgere attività che non rientrano tra i compiti istituzionali può essere consentito ai dipendenti per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro purchè contenuta nei tempi strettamente necessari allo svolgimento di tali transazioni (ad esempio, per effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e assicurativi).

Utilizzo di telefoni, scanner e fotocopiatrici

- Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di necessità ed urgenza, mediante il telefono fisso aziendale a disposizione.
- Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per I 'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite digitando il prefisso per l' addebito delle chiamate personali.
- È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa autorizzazione da parte del Responsabile dell'unità operativa.

- È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva autorizzazione da parte del Responsabile dell'unità operativa.
- È vietato l'utilizzo di scanner aziendali per fini personali, salvo preventiva autorizzazione da parte del Responsabile dell'unità operativa.
- Solo in caso di necessità e urgenza, gli Utenti possono utilizzare tali beni per motivi non attinenti l'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati.
- Il controllo sul corretto utilizzo degli strumenti in parola è affidato al Responsabile della unità operativa a cui detti strumenti sono stati assegnati.

Protezione antivirus

- Il sistema informatico dell'Azienda è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software di tipo malware
- Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l' accaduto alla divisione IT.
- Ogni dispositivo di supporto di memorizzazione elettronico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale dalla divisione IT.
- L'utente utilizzatore del PC verifica periodicamente lo stato di aggiornamento dell'antivirus aziendale installato. A fronte di eventuali anomalie contatta la divisione IT.

Controlli

- L'articolo 23 del recente D.lgs. 14 settembre 2015 n. 151 (così detto "Decreto sulle semplificazioni" attuativo della Legge delega 10.12.2014 n. 183, anche nota come "legge di riforma del diritto del lavoro" o "Jobs Act") ha modificato il contenuto dell'articolo 4 della Legge 300/1970, ora rubricato "Impianti audiovisivi e altri strumenti di controllo".
- Il testo del nuovo articolo 4 della Legge 300/1970, nel confermare, al primo comma, la disciplina applicabile agli strumenti di controllo a distanza dell'attività dei lavoratori necessari per esigenze organizzative e produttive, per

la sicurezza del lavoro e per la tutela del patrimonio aziendale (come le telecamere o i rilevatori di posizione Gps), che rimangono sottoposti alla stessa disciplina di divieti e di controlli di prima, ha introdotto, al comma due, una disciplina diversa per quanto concerne i dispositivi utilizzati dal lavoratore per rendere la prestazione lavorativa (computer, tablet, telefoni, smartphone) stabilendo espressamente che "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. Le informazioni raccolte a 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 D.lgs. 30 giugno 2003 n. 196

- Alla luce delle disposizioni dettate dal succitato D.lgs. 151/2015, l'Azienda può effettuare controlli sugli strumenti informatici utilizzati dal lavoratore per rendere la prestazione lavorativa (personal computer, tablet, telefoni e smartphone), senza la necessità di accordi sindacali preventivi e fornendo al lavoratore un'adeguata informativa sulle regole previste per l'utilizzo lavorativo ed eventualmente personale degli strumenti di cui si tratta e sulle modalità e i casi in cui potranno effettuarsi i controlli.
- Si dà atto che l'informativa ai lavoratori, di cui al precedente capoverso, viene garantita dall'Azienda mediante la diffusione del presente Regolamento, approvato con delibera del Direttore Generale/Commissario, e che le informazioni raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro nel rispetto di quanto previsto dal "Codice della privacy" (D.lgs. 196/2003)
- In ottemperanza a quanto stabilito dall'art. 4 del d.lgs. 300/1970, non vengono nel modo più assoluto utilizzate apparecchiature/strumentazioni hardware e software al fine di consentire controlli a distanza, prolungati, costanti o indiscriminati dei lavoratori. È quindi nel pieno rispetto dei principi di pertinenza e di non eccedenza ed evitando ogni interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, che l'Azienda si riserva di effettuare controlli sull'uso degli strumenti ICT. Detti controlli sono svolti esclusivamente dalla Struttura competente per la gestione dei sistemi informativi. I controlli effettuati di routine sono indiretti e di tipo aggregato. In particolare detti controlli sono finalizzati a verificare la funzionalità e la sicurezza dei sistemi. Controlli indiretti di tipo aggregato, ma più specifici, vengono altresì attivati in caso di rilevamento di anomalie nell'utilizzo delle

apparecchiature ICT. Qualora la anomalia dovesse ripetersi e riguardare lo stesso ambito lavorativo si procederà con l'effettuazione di controlli più puntuali e su base individuale secondo le modalità indicate al successivo punto

Graduazione dei controlli

- Premesso che "il dipendente deve utilizzare il materiale o le attrezzature di cui dispone per ragioni di ufficio e i servizi telematici e telefonici dell'ufficio nel rispetto dei vincoli posti dall'amministrazione" (art. 11, Codice di comportamento dei dipendenti pubblici), come stabilito dal Garante della privacy nelle già citate "Linee guida per posta elettronica e internet" del 01.03.2007, all'articolo 6.1. rubricato "Graduazione", nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
- Come stabilito altresì' dalla già citata Direttiva n. 2/2009 ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro", l'eventuale controllo è lecito solo se sono rispettati i principi di proporzionalità, pertinenza e non eccedenza nelle attività di controllo. Le limitazioni della libertà e dei diritti individuali devono essere proporzionate allo scopo perseguito ed è, in ogni caso, esclusa l'ammissibilità di controlli prolungati, costanti e indiscriminati.
- Per quanto possibile deve essere preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.
- Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite.
- L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Utilizzo di social networks

Al fine di assicurare il rispetto del segreto d'ufficio, del segreto professionale e della riservatezza dei dati conosciuti in ambito aziendale, è vietato l'uso, anche

privato, dei social networks per lo scambio di informazioni e dati inerenti l'attività istituzionale.

Entrata in vigore e pubblicità

Le regole contenute nel presente atto entrano in vigore dalla data di adozione del provvedimento di approvazione. Del presente atto sarà fornita massima pubblicità e diffusione mediante la sua pubblicazione nel sito internet aziendale, nell'l'intranet aziendale e nel Portale Trasparenza di Ales.

Disposizioni finali

Per quanto non espressamente richiamato nel presente atto, si rinvia alle disposizioni civili e penali vigenti in materia.

Monitoraggio e controlli

Ales tal fine si avvale legittimamente di sistemi che consentono indirettamente un controllo di eventi potenzialmente pericolosi sulla rete. Non saranno utilizzati sistemi hardware e/o software idonei ad effettuare un controllo a distanza dei lavoratori, in particolare mediante:

1. la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
2. la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
3. la lettura o la registrazione dei caratteri inseriti tramite la tastiera e analogo dispositivo. Sono comunque esclusi controlli prolungati, costanti e/o indiscriminati.
4. Le attività sull'uso del servizio di accesso ad internet e all'accesso ai servizi informatici vengano automaticamente registrate in forma elettronica (LOG) Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività. I dati personali contenuti nei LOG possono essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
- quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
- ove richiesti dal Presidente e Amministratore delegato o DPO a seguito di segnalazione scritta e motivata da parte di un dirigente che abbia ravvisato o presuma, sulla base di gravi indizi, comportamenti di un dipendente o collaboratore ad esso assegnati, in qualsiasi modo non conformi a quanto previsto dal presente disciplinare.

I dati contenuti nei LOG sono conservati per il tempo strettamente necessario al perseguimento di:

- finalità organizzative, produttive e di sicurezza, comunque non superiore a una settimana lavorativa, e sono periodicamente cancellati automaticamente dal sistema. Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e avverrà 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 e della polizia giudiziaria.

In questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità esplicitati. I dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell'utente che ha effettuato l'installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

Interruzione e cessazione del servizio

Eventuali interruzioni del servizio sono comunicate agli utenti. L'utilizzo del servizio di accesso alla rete ed al sistema informatico di Ales viene disabilitato previa comunicazione alla mail: it@ales-spa.com quando, per una qualunque ragione, viene

interrotto il rapporto lavorativo con Ales il giorno successivo a quello della scadenza del contratto.

Responsabilità e sanzioni

L'utente delle risorse informatiche di Ales che abbia violato il presente regolamento o la normativa ivi richiamata, potrà essere soggetto ad azione disciplinare in conformità a quanto stabilito dal contratto collettivo nonchè dal Codice disciplinare e di comportamento di Ales fatta salva la possibilità per Ales di esercitare le opportune azioni giudiziarie nelle sedi competenti, a tutela dei propri diritti giuridicamente tutelati. In caso di danno, la violazione espone altresì l'utente responsabile ad azioni legali di carattere civile o penale da parte dei danneggiati e a richieste di risarcimento anche da parte di Ales.

Glossario

Backup: il termine, che significa copia di sicurezza, indica l'operazione di duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server. Normalmente viene svolta con una periodicità stabilita.

Chat: (letteralmente, "chiacchierata") è un servizio informatico che permette attraverso internet, di attivare e gestire un dialogo in tempo reale fra due o più utenti utilizzando principalmente messaggi testuali.

File sharing: condivisione di file all'interno di una rete comune.

Forum: generalmente si riferisce ad un archivio informatico contenente discussioni e messaggi scritti dagli utenti oppure al software utilizzato per fornire questo archivio. Ci si riferisce comunemente ai forum anche come board, message board, bulletin board, gruppi di discussione, bacheche e simili.

Guestbook: (letteralmente, libro degli ospiti) è un servizio interattivo che permette ai visitatori di un sito web di poter lasciare 'firme' e commenti.

ID utente: codice identificativo personale per l'accesso ai sistemi informatici. Normalmente è formato dal cognome o dal cognome e parte del nome.

LOG: il termine, che significa giornale di bordo o semplicemente giornale, viene utilizzato nell'informatica per indicare la registrazione cronologica delle operazioni man mano che vengono eseguite ed il file su cui tali registrazioni sono memorizzate.

Mailing-list: (letteralmente, lista per corrispondenza traducibile in italiano con lista di diffusione) è un sistema organizzato per la partecipazione di più persone in una discussione tramite posta elettronica.

Mail spamming: è l'invio di grandi quantità di messaggi indesiderati (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è internet attraverso l'e-mail.

Password: (in italiano: “parola chiave”, “parola d'ordine”, o anche “parola d'accesso”) è una sequenza di caratteri utilizzata per accedere ad una risorsa informatica.

Podcasting: sistema che permette di scaricare in modo automatico documenti (generalmente audio o video) chiamati podcast, utilizzando un programma generalmente gratuito chiamato aggregatore o feeder. Con podcast si intende un file (generalmente audio o video), messo a disposizione su Internet e scaricabile automaticamente.

Software freeware: programmi software distribuiti in modo gratuito.

Software peer-to-peer: programmi utilizzati per la condivisione e lo scambio di files fra elaboratori. Questi programmi vengono utilizzati principalmente per scambiarsi file di tipo mp3,(file musicali) e DivX (contenenti i film) spesso in violazione dei diritti d'autore.

Stand - alone: si riferisce ad un’apparecchiatura capace di funzionare da sola, indipendentemente dalla presenza di altre apparecchiature con cui potrebbe comunque interagire.

Streaming: identifica un flusso di dati audio/video trasmessi da una sorgente a una o più destinazioni tramite una rete telematica. Questi dati vengono riprodotti man mano che arrivano a destinazione.

Webcast/Webcasting: descrive la trasmissione di segnale audio o video, in tempo reale o ritardato, mediante tecnologie web. Il suono o il video sono catturati con sistemi audio-video convenzionali, quindi digitalizzati e inviati in streaming su un web

server. Un client webcast consente agli utenti di connettersi ad un server che sta distribuendo (operazione detta di webcasting) e di ascoltare o visualizzare il contenuto audio/video .