Insula

Insula spa
società soggetta alla
direzione e coordinamento
del Comune di Venezia

Regolamento per l'utilizzo dei sistemi e strumenti informatici

luglio 2023

Premessa

La diffusione di tecnologie informatiche sempre più nuove e il libero accesso alla rete internet da personal computer, tablet e smartphone, espone Insula e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e disciplina sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine della società stessa.
Peraltro, anche lo sviluppo delle reti sociali on line incide, direttamente o indirettamente, sulle attività della società, sulla sua immagine e sulle relazioni instaurate. Risulta pertanto necessario che, al fine di evitare il sorgere di rischi derivanti dalla presenza della denominazione di Insula e/o di altri riferimenti ad essa riconducibili, anche solo indiretta, sui social media, si tenga parimenti conto di questo preciso aspetto nel presente Regolamento.
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, Insula ha adottato un Regolamento interno diretto ad evitare che comportamenti, anche inconsapevoli, possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e quindi del proprio sistema informatico. Il Regolamento svolge anche la funzione di informare compiutamente gli utenti riguardo i trattamenti specifici dei loro dati personali che vengono effettuati e sulle modalità adottate.
Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni fornite a tutti gli incaricati o persone autorizzate al trattamento, in attuazione del Regolamento UE 2016/679 (di seguito il "GDPR") contenenti anche le misure di sicurezza, nonché integrano le informazioni agli interessati ai sensi dell'art. 13 del GDPR, anche in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse, come previsto dall'art. 4, comma 3, dello Statuto dei lavoratori.
Considerato inoltre che Insula, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, fornisce ai propri dipendenti che ne necessitino per il tipo di funzioni svolte, telefoni cellulari, computer portatili, smartphone, ecc., sono state inserite nel Regolamento alcune clausole relative alle modalità ed ai doveri che ciascun dipendente deve osservare nell'utilizzo di tale strumentazione.

Entrata in vigore del Regolamento e pubblicità

1. Il nuovo Regolamento entrerà in vigore il giorno 1° settembre 2023. Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate, qualora incompatibili o difformi, poiché sostituite dalle presenti.
2. Copia del Regolamento, oltre ad essere pubblicata nella cartella della bacheca aziendale presente nel server della società (sezione "public"), come previsto dall'art. 7 della Legge n. 300/1970, verrà consegnata a ciascun dipendente, anche ai fini dell'art. 13 del GDPR e dell'art. 4, comma 3, dello Statuto dei lavoratori, e verrà altresì consegnata ai vari collaboratori, consulenti, agenti od altri incaricati esterni (es. incaricati software house, incaricati dei professionisti di cui si avvale la società, ecc.) che venissero autorizzati a far uso di strumenti tecnologici della società o ad accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, il presente Regolamento entra a far parte, per quanto occorra, del Codice disciplinare aziendale.

Campo di applicazione del Regolamento

1. Il nuovo Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori e consulenti di Insula a prescindere dal rapporto contrattuale intrattenuto (lavoratori somministrati, collaboratori coordinati e continuativi, in stage, agenti di commercio, prestatori d'opera intellettuale, ecc.) che venissero autorizzati a far uso di strumenti tecnologici della società o perfino ad accedere alla rete informatica aziendale o ad

eventuali dati ed informazioni ivi conservati e trattati. Pertanto, le regole di seguito previste devono intendersi a carico tanto dei primi quanto dei secondi, ferma restando la necessità che si dia opportuno conto del presente Regolamento nel contratto concluso con quest'ultimi. Le disposizioni del presente Regolamento si applicano anche ai lavoratori che eseguono la prestazione lavorativa, parzialmente od esclusivamente, a tempo determinato od indeterminato, in modalità di "lavoro agile", a norma degli articoli dal n. 18 al n. 23 del D.lgs. n. 231/2017, eventualmente integrate da ulteriori prescrizioni fornite allo stesso lavoratore in occasione dell'avvio dello "smart working".

2. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve così intendersi ogni dipendente, collaboratore e/o consulente (come sopra già precisato) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "responsabile del trattamento" o "incaricato o persona autorizzata al trattamento", ai fini del Regolamento generale n. 679/2016, in ragione delle attività e degli impegni che si assume nell'organizzazione aziendale od a favore della società stessa.

Utilizzo del personal computer

1. Il personal computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.
2. Il personal computer dato in affidamento all'utente permette l'accesso alla rete di Insula solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto del presente Regolamento sull'assegnazione delle credenziali.
3. Insula rende noto che il personale incaricato che opera per il servizio Information and Communication Technology (nel seguito per brevità "servizio ICT") della stessa Insula è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività della società, si applica anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il servizio ICT ne darà comunicazione agli utenti interessati, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso.
4. Il personale incaricato del servizio ICT ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, ecc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.
5. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del servizio ICT per conto di Insula né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la stessa Insula a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico di Insula, come disposto dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.
6. Salvo preventiva espressa autorizzazione del personale del servizio ICT, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, unità di memoria esterne, ecc.).
7. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo

immediatamente il personale del servizio ICT nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

8. Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Gestione e assegnazione delle credenziali di autenticazione

1. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale incaricato del servizio ICT, previa espressa indicazione della direzione aziendale ovvero previa formale richiesta del responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal servizio ICT, associato ad una parola chiave (password) riservata, che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del servizio ICT.
3. La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
4. È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, ogni volta che il sistema comunichi la scadenza della stessa. Il sistema infatti assegna di default un termine di validità delle password. Qualora l'utente non provveda a variare la propria password in tempo, l'accesso al personale computer e/o al sistema verrà temporaneamente bloccato.
5. Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del servizio ICT.
6. Soggetto preposto alla custodia delle credenziali di autenticazione è il personale incaricato del servizio ICT di Insula.

Utilizzo della rete di Insula

1. Per l'accesso alla rete di Insula ciascun utente deve utilizzare le proprie credenziali di autenticazione. Lì dove sia possibile accedere alla rete aziendale da remoto, con accesso anche ai dati attinenti all'attività dell'utente presenti nel server ed alla sua casella posta elettronica, questo potrà avvenire solo a seguito di autorizzata installazione e configurazione nel proprio pc portatile (personale od in dotazione) di apposita VPN aziendale e mediante le proprie credenziali di autenticazione (od altra credenziale assegnata dal personale del servizio ICT), o mediante sistemi di connessione che garantiscano un livello idoneo di sicurezza .
2. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
3. Le cartelle utenti presenti nei server di Insula sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e back up da parte del personale del servizio ICT. Si ricorda che tutti i dischi o altre unità di memorizzazione locali - es. disco C: interno PC - non sono soggette a salvataggio da parte del personale incaricato del servizio ICT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

4. Il personale del servizio ICT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.
5. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.
6. Nella gestione dei sistemi informatici aziendali, il servizio ICT potrà acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali, ad esempio, le informazioni sugli orari di accensione e spegnimento dei personal computer, rilevati automaticamente tramite il sistema di autenticazione al dominio di rete, e i log degli accessi a specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate, ai sensi del successivo punto sull'osservanza delle disposizioni in materia di privacy, per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate nel precedente terzo paragrafo sull'utilizzo del personale computer, e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.
7. L'utente è infine tenuto a far uso degli applicativi riferibili alle piattaforme di comunicazione e condivisione di documenti appositamente installate dal servizio ICT. In tal senso, non potrà avvalersi, anche nelle comunicazioni con i terzi esterni alla società, di piattaforme non preventivamente valutate, anche sotto il profilo della sicurezza, dal servizio ICT.

Utilizzo di altri dispositivi elettronici

1. Tutti i dispositivi elettronici dati in dotazione al personale di Insula devono considerarsi strumenti di lavoro: ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative. Fra i dispositivi in questione vanno annoverati i telefoni aziendali, PC portatili, tablet, telefoni cellulari, smartphone, ecc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere alla rete di Insula o di condividere documenti, dati e materiali ivi conservati e/o trattati.
2. L'utente resta responsabile del singolo dispositivo assegnato e deve custodirlo con diligenza sia durante trasferte e spostamenti sia durante l'utilizzo nel luogo di lavoro; va sempre adottata ogni cautela per evitare danni o sottrazioni. In caso di smarrimento o furto di dispositivi le cui memorie possano essere cancellate o bloccate da remoto a cura del servizio ICT per evitare sottrazioni o diffusioni di dati incontrollati, l'utente dovrà immediatamente avvisare la direzione aziendale ed il servizio ICT, e comunque al massimo entro la giornata in cui è avvenuto il fatto, via mail.
3. Con riferimento ai telefoni aziendali e telefoni cellulari, fermo restando quanto sopra già disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, viene consentita solo nel caso di comprovata necessità ed urgenza.
4. Al dipendente assegnatario di telefonia mobile è fatto espresso divieto di:
   - rimuovere la sim dal telefono mobile aziendale per installarla su apparecchio diverso rispetto a quello assegnato;
   - utilizzare il telefono in dotazione per uso personale o comunque per fini diversi da quelli aziendali, salvo l'abilitazione all'addebito personale;
   - utilizzare la connessione internet ovvero la gestione di messaggi di posta elettronica per gli apparecchi dotati delle citate funzionalità per scopi differenti da quelli lavorativi.

   Insula si riserva comunque la possibilità di effettuare controlli sull'andamento dei consumi. La società si riserva altresì il diritto di verificare le fatturazioni concernenti le chiamate in uscita compiute dal dipendente, oltre alle sole in entrata in roaming se dovessero comportare un costo per l'azienda stessa, ai soli fini di riduzione dei costi aziendali e di verifica dell'adeguatezza del contratto sottoscritto con il fornitore dei servizi telefonici. La conservazione dei dati relativi al traffico telefonico verrà conservata per sei mesi; la società procederà infine, per quanto possibile, all'anonimizzazione dei dati in questione.

5. Si precisa, peraltro, che le disposizioni previste nel presente Regolamento trovano applicazione anche nell'uso dei dispositivi elettronici qui considerati.
6. Viene infine disposto il divieto di utilizzo per fini personali della strumentazione aziendale, ivi comprese le fotocopiatrici, salva diversa esplicita autorizzazione da parte del responsabile di ufficio.
7. Ferma restando la gestione della specifica sicurezza informatica, posta in capo al personale del servizio ICT, ogni utente del sistema di stampanti in rete deve adottare comportamenti atti a proteggere il know-how aziendale e alla riservatezza dei dati personali. Si deve, quindi, evitare di lasciare abbandonate le stampe presso la stampante, stampe che devono essere ritirate tempestivamente. In caso di scannerizzazione di documenti cartacei, l'invio all'esterno tramite la stessa stampante in rete deve essere motivato da esigenze lavorative e, nel caso di contenuti riservati (contraddistinti dalla dicitura "strettamente riservati" o analoghe apposte sul documento) deve essere autorizzato dal responsabile di ufficio.

Utilizzo e conservazione dei supporti rimovibili

1. Tutti i supporti magnetici rimovibili CD e DVD riscrivibili, supporti USB, ecc., contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
2. L'utente resta in ogni caso responsabile della custodia dei supporti e dei dati aziendali in essi contenuti; in particolare, i supporti contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.
3. Viene severamente vietato l'utilizzo di supporti rimovibili personali.
4. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del servizio ICT e seguire le istruzioni da questo impartite. Nel caso di dispositivi elettronici, con riferimento in particolare a PC portatili, tablet ed altri dispositivi sui quali possano venir salvati documenti, dati ed altro materiale, dovrà farsi particolare attenzione al salvataggio in opportuni supporti esterni di tale materiale oppure alla sua rimozione effettiva prima della riconsegna del dispositivo, concordata comunque ogni opportuna azione al riguardo con il personale del servizio ICT.

Uso della posta elettronica

1. La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le archiviazioni dei messaggi avvengono su server in disponibilità di Insula. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
2. È fatto divieto di utilizzare le caselle di posta elettronica nome.cognome@nomeazienda.it per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
   - l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
   - l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing list;
   - la partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del servizio ICT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
3. Poiché la casella di posta assegnata costituisce strumento di lavoro, è opportuno evidenziare che i messaggi ivi contenuti, verranno conservati nei server in disponibilità della società stessa per 10 anni, a norma dell'art. 2220 del Codice civile. I messaggi privi di valenza commerciale o lavorativa, di conseguenza, dovranno essere selezionati e periodicamente cancellati a cura ed onere dell'utente della casella.
4. In ogni caso, la casella di posta deve essere mantenuta in ordine, cancellando documenti inutili (anche allegati ingombranti., o non costituenti corrispondenza commerciale e lavorativa che, come tale, deve essere sottoposta al sistema di gestione documentale aziendale come

disposto al precedente punto. In caso di cessazione del rapporto di lavoro, il singolo dipendente è tenuto ad eliminare dalle proprie cartelle tutti i messaggi di posta elettronica ed i documenti non pertinenti l'attività aziendale e non utili alle esigenze aziendali, mantenendo integra, invece, tutta la corrispondenza e documentazione inerente all'attività lavorativa. Resta inteso che, di conseguenza, la documentazione presente nel profilo del singolo utente che cessa il rapporto di lavoro verrà considerata presuntivamente dalla società quale corrispondenza e documentazione lavorativa e non personale.

5. È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.
6. È obbligatorio porre la massima attenzione nell'aprire i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti web o ftp non conosciuti).
7. Al fine di garantire il regolare svolgimento dei servizi, in caso di assenza non programmata (ad es. per malattia) che si protraggano oltre la settimana, sarà consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dalla società, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario.
8. Il personale del servizio ICT potrà accedere alla casella di posta elettronica in caso di assenza prolungata o impedimento dell'utente solo se considerato indispensabile ed indifferibile per esclusive finalità di operatività e sicurezza del sistema, informando successivamente lo stesso utente.
9. Insula si riserva la facoltà, a proprio insindacabile giudizio, di assegnare o ritirare l'utilizzo della casella di posta elettronica in base alla propria esclusiva e insindacabile valutazione della necessità di utilizzo della stessa per lo svolgimento delle attività lavorative. Di ogni eventuale disattivazione o sospensione della casella di posta elettronica assegnata verrà data informativa al singolo interessato.
10. La casella di posta elettronica, unitamente alle credenziali di autenticazione per l'accesso alla rete, viene disattivata al momento della conclusione del rapporto di lavoro che ne giustificava l'assegnazione. Contestualmente alla disattivazione:
    - verrà in automatico generata una mail ai mittenti di mancato inoltro e con indicazione della diversa casella di posta elettronica aziendale cui trasmettere i messaggi da recapitare;
    - viene escluso, comunque, l'invio di messaggi da tale casella di posta.
11. Nel caso in cui venisse assegnato all'utente anche la gestione di uno o più indirizzi di posta elettronica certificata di cui la società si fosse dotata, tale utente dovrà attenersi alle regole previste nell'ulteriore apposito Regolamento aziendale a ciò dedicato e che va comunque a completare ed integrare il presente Regolamento.
12. Nel caso di invio di messaggi rivolti a più persone sarà necessario valutare con attenzione se è lecito che ogni destinatario venga a conoscenza di quali altri destinatari sono coinvolti. Si sottolinea che, ove necessario al fine di garantire la riservatezza dei singoli destinatari, gli indirizzi dei destinatari devono essere inseriti in copia nascosta (ccn).

Navigazione in Internet

1. Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
2. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:
    - l'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del servizio ICT);
    - l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on line e simili, fatti salvi i casi direttamente autorizzati dalla direzione generale (o eventualmente dal responsabile d'ufficio e/o del servizio ICT) e comunque nel rispetto delle normali procedure di acquisto;
    - ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività

lavorativa
- la partecipazione a Forum non professionali, l'iscrizione con account aziendale e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

3. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, Insula rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una "black list".
4. Gli eventuali controlli, compiuti dal personale incaricato del servizio ICT ai sensi del precedente punto 3.3, potranno avvenire mediante un sistema di controllo dei contenuti (proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre sei mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza della società.
5. L'utilizzo di tutte le reti wi-fi eventualmente presenti in azienda è limitato agli utenti autorizzati. A tale scopo si precisa che l'utilizzo di qualsiasi rete wi-fi disponibile in azienda e dalla stessa configurata è possibile solo a seguito di digitazione di specifiche credenziali che vengono assegnate dal responsabile/servizio ICT.
6. L'accesso da remoto alla rete aziendale è possibile agli utenti abilitati solo a seguito di comunicazione di specifiche credenziali o dell'installazione di software che lo abilita sui dispositivi in uso.
7. L'accesso da remoto alla rete aziendale è possibile solo utilizzando i dispositivi previsti. A tale scopo vengono svolti controlli automatici che impediscono l'accesso utilizzando dispositivi non abilitati.

Protezione antivirus

1. Il sistema informatico di Insula è protetto da software antivirus aggiornato periodicamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
2. 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 al personale del servizio ICT.
3. Ogni dispositivo magnetico di provenienza esterna alla società dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del servizio ICT.

Partecipazioni a social media

1. L'eventuale utilizzo ai fini aziendali dei social media – quali Facebook™, Twitter™, Linkedin™, Instagram™, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dalla società attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti (conformemente a quanto disposto al precedente punto sulla navigazione in internet).
2. Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, Insula ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio aziendale, anche immateriale, quanto i propri collaboratori, i propri utenti e gli enti committenti, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che viene vietata la partecipazione agli stessi social media durante l'orario di lavoro. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione da Insula, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti della stessa società.
3. La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate da Insula riservate ed in genere, a titolo

esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, programmatiche, sui fornitori ed altri soggetti che ordinariamente hanno contatti con gli uffici della società stessa.

4. L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali.
5. L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso la società, i colleghi, i soci, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito aziendale.
6. Infine, in via generale ed ove non autorizzato in senso diverso dal proprio responsabile d'ufficio, l'utente, nell'uso dei social network, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con la società, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili ad Insula.

Osservanza delle disposizioni in materia di privacy

1. È obbligatorio attenersi alle disposizioni in materia di privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato o persona autorizzata al trattamento dei dati ai sensi del Regolamento generale UE 2016/679.
2. Gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma 2, della Legge n. 300/1970; conseguentemente, le informazioni raccolte sulla base di quanto indicato nel Regolamento, anche conformemente al successivo punto, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti (conformemente al successivo punto su incidenti e data breach), fermo restando il rispetto della normativa in materia di protezione dei dati personali.
3. Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, Insula provvederà conformemente a quanto disposto dall'art. 4, comma 1, della Legge n. 300/1970, dandone anche opportuna informazione agli utenti stessi.

Accesso ai dati trattati dall'utente

Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.), per finalità di controllo e programmazione dei costi aziendali (es. verifica costi di connessione ad internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della direzione aziendale, tramite il personale del servizio ICT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy e delle procedure di cui ai precedenti a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

Incidenti e data breach

1. In riferimento a quanto indicato al precedente punto sulla protezione antivirus, ogni malfunzionamento o anomalia del sistema informatico e dei dispositivi assegnati deve essere tempestivamente segnalato al servizio ICT per gli eventuali interventi tecnici e di protezione del sistema.
2. In caso di incidenti che possono determinare una violazione di dati personali ("data breach"), l'utente dovrà immediatamente comunicare la possibile violazione al servizio ICT, al fine di permettere a Insula di attivare la procedura aziendale di verifica degli eventi e di adempiere, se del caso, agli obblighi di notifica e di comunicazione previsti dagli articoli n. 33 e 34 del Regolamento UE 2016/679 a carico del titolare del trattamento. Si tenga a mente che per "data breach" ai sensi del GDPR si intende qualsiasi violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso abusivo (cioè non autorizzato) ai dati personali gestiti dalla società, siano essi archiviati, trasmessi o comunque in altro modo trattati.

Sistemi di controlli graduali

1. In caso di anomalie, il personale incaricato del servizio ICT effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base più ristretta o anche individuale potranno essere computi solo in caso di successive ulteriori anomalie.
2. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL.

Aggiornamento e revisione

1. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla direzione generale.
2. Il presente Regolamento è soggetto periodicamente a revisione.