REG TEC 01 Veritas spa

Regolamento interno per l'utilizzo del sistema informatico

Conforme alla norma UNI EN ISO 9001:2015
Conforme alla norma UNI EN ISO 14001:2015
Componente del Modello organizzativo ex dlgs 231/2001
Conforme al Regolamento UE 2016/679

VERITAS

Indice

Preparazione	Verifica	Approvazione
Contenzioso del lavoro e disciplina *Laura Meggiorato* *(FIRMATO)*	Direttore Risorse umane e organizzazione di Gruppo *Chiara Bellon* *(FIRMATO)*	Direttore Generale *Andrea Razzini* *(FIRMATO)*
Sistemi informativi *Luana Cappelletto* *(FIRMATO)*	Direttore Patrimonio servizi per l'utenza e bollettazione di Gruppo *Maurizio Calligaro* *(FIRMATO)*	
	Qualità Ambiente e Sicurezza *Giuliana Da Villa* *(FIRMATO)*	
	Direttore Amministrazione, finanza e pianificazione e controllo di Gruppo *Massimiliano Hiche* *(FIRMATO)*	

Variazioni: modifica il regolamento informatico in vigore alla luce della nuova normativa in materia di privacy GDPR (Regolamento UE 2016/679).

1 Premessa

La progressiva diffusione delle tecnologie informatiche, e in particolare il libero accesso alla rete internet dai personal computer aziendali, espone Veritas spa e le società del Gruppo che utilizzano in service i sistemi informativi della controllante, a rischi di carattere patrimoniale e a responsabilità penali con conseguenti ricadute in termini di sicurezza e di immagine dell'azienda.
Per tali motivi l'utilizzo delle risorse informatiche e telematiche fornite a Veritas spa deve ispirarsi ai principi di ***diligenza***, **correttezza** e ***buona fede*** (principi questi che sono comunque sottesi al rapporto di lavoro) nel giusto contemperamento anche degli obblighi derivanti dall'applicazione del regolamento UE 2016/679.
Veritas spa ha dunque adottato il presente Regolamento al fine di prevenire, ancorché a evitare, che comportamenti anche inconsapevoli, possano minacciare o compromettere la sicurezza nel trattamento dei dati o che comportamenti impropri distolgano le risorse aziendali dall'uso cui sono deputate.

2 Scopo

Il presente Regolamento definisce le modalità di utilizzo dei sistemi informativi aziendali, disciplinando il corretto utilizzo degli strumenti informatici, telematici e telefonici da parte dei dipendenti di Veritas spa e degli altri soggetti autorizzati, anche al fine della prevenzione dei crimini informatici così come previsti dal dlgs 231/01 (art. 24 bis) ovvero dei comportamenti impropri o illeciti compiuti sulla rete aziendale tramite l'utilizzo delle dotazioni informatiche.
Il presente Regolamento, comprensivo del Modello di consenso informato consegnato al dipendente al momento di assegnazione delle dotazioni informatiche e/o telematiche necessarie a rendere la prestazione lavorativa (allegato "A" al presente Regolamento), è da considerarsi, unitamente alla specifica informativa ex art. 4, co. 2 della legge 300/70 così come novellato dal dlgs 151/2015, la policy aziendale in materia di utilizzo corretto e consapevole delle dotazioni informatiche e telematiche assegnate.

3 Campo di applicazione

Destinatari del presente regolamento sono tutti coloro cui viene consentito l'accesso, a vario titolo, alla rete di Veritas spa.

4 Utilizzo di dotazioni e strumenti informatici

Con il termine strumenti informatici si intendono tutte le attrezzature hardware e software, quali personal computer, computer portatili, tablet, cellulari e altri strumenti dedicati all'utilizzo dei servizi informatici del gruppo Veritas spa ed esterni al gruppo Veritas spa (ivi compresi indirizzi di posta elettronica, pec, firme digitali ecc.)
Tali strumenti, da considerarsi necessari a rendere la prestazione lavorativa, devono esser utilizzati a soli scopi lavorativi considerato che i dati, seppur raccolti in base ai principi di necessità e proporzionalità rispetto al fine perseguito, potranno essere utilizzati per tutti i fini connessi al rapporto di lavoro, compresi quelli disciplinari.
Nel particolare caso di telefoni cellulari, utilizzati anche a titolo personale, vale quanto riportato nel successivo paragrafo "Utilizzo dei dispositivi mobili".
Le richieste di nuove dotazioni, assistenza, riparazione e sostituzione vanno inoltrate all'ufficio Sistemi informativi tramite portale D9 (Delta 9).
I dipendenti dotati di strumenti informatici sono responsabili della loro custodia e utilizzo, secondo quanto previsto dalle disposizioni degli specifici articoli del presente Regolamento. Il dipendente che, venendo meno

al dovere di diligenza nella custodia, causi il danneggiamento o smarrimento delle dotazioni informatiche affidate, risponderà del danno patrimoniale e/o non patrimoniale arrecato a Veritas spa e/o a terzi secondo quanto previsto dal codice disciplinare e dai documenti in esso richiamati.
I dipendenti sono tenuti a comunicare tempestivamente all'ufficio Sistemi informativi eventuali furti, e/o danneggiamenti, di tali strumenti, nonché eventuali anomalie di funzionamento che ne possano pregiudicare la regolare funzionalità. Nel caso di furto o smarrimento di un qualsiasi dispositivo appartenente a Veritas spa il dipendente che ne abbia conoscenza, deve:

- sporgere denuncia, entro 24 ore dal furto o dallo smarrimento, presso le forze dell'ordine quali polizia o carabinieri (specificando il codice IMEI nel caso di cellulari o di SIM inserita all'interno del tablet o portatile);
- richiedere il blocco SIM all'operatore telefonico;
- informare immediatamente, formalizzando successivamente la comunicazione attraverso la modalità Delta9, l'Ufficio sistemi informativi anche ai fini della tenuta, da parte dell'ufficio stesso, del registro violazione rete e violazione dati". Sarà quindi cura dell'ufficio Sistemi informativi comunicare all'ufficio Privacy l'accadimento in modo che lo stesso possa effettuare ogni valutazione del contenuto del dispositivo rubato o smarrito a fini della eventuale necessità di attivazione delle procedure previste dalla normativa europea in materia di privacy;
- nel caso – per qualsivoglia motivo – fosse impossibile prendere contatti immediati con l'ufficio Sistemi informativi, il dipendente dovrà informare dell'accaduto il responsabile dell'ufficio Privacy. In tale fattispecie sarà quest'ultimo a contattare poi l'ufficio Sistemi informativi per attivare le procedure conseguenti;
- richiedere una nuova dotazione informatica allegando la denuncia alle forze dell'ordine.

Quanto sopra riportato al fine di evitare violazioni della sicurezza dei dati contenuti nei sopra indicati dispositivi che possano comportare, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato a tali dati.
Una volta acquisita la denuncia di furto o smarrimento, l'ufficio Sistemi informativi potrà procedere al "reset" del dispositivo se e in quanto raggiungibile da remoto.

4.1 Accesso documenti aziendali

Tutti i documenti aziendali vanno collocati esclusivamente nelle apposite condivisioni di rete (DFS), per le quali viene eseguito regolare backup e monitorato l'accesso (log Amministratori). Non è consentito memorizzare documenti aziendali su dispositivi esterni (chiavette USB, hard disk mobili, cloud personali ecc.)
Le abilitazioni degli utenti alle singole folder di pertinenza vanno formalizzate con un ticket D9 da parte del responsabile d'area.
Non è consentito utilizzare i PC per memorizzare documenti aziendali, se non delle copie per uso temporaneo.
Non viene effettuato alcun backup delle postazioni client (PC, tablet, laptop) né tantomeno gestito il trasferimento dei dati locali della postazione, in caso di sostituzione del PC.

4.2 Accesso internet

Ogni accesso alla rete internet deve essere richiesto e autorizzato da parte del Dirigente competente attraverso il portale interno D9. L'ufficio Sistemi informativi provvede all'attivazione del servizio.
Gli accessi temporanei alla navigazione internet tramite rete aziendale per consulenti e fornitori vanno comunque tracciati tramite ticket su D9, allegando il modulo consenso informato sottoscritto dall'interessato.
Al dipendente che, per motivi organizzativi, venga trasferito ad altro settore e/o ufficio ovvero modifichi le proprie mansioni, verrà automaticamente inibito l'accesso al servizio internet aziendale. Sarà cura del nuovo Dirigente e/o del diverso diretto responsabile, richiedere all'ufficio Sistemi informativi un nuovo accesso.
Veritas spa riconosce la possibilità ai destinatari del presente Regolamento di utilizzare le dotazioni aziendali

assegnate, anche per fini personali, purché nel rispetto delle prescrizioni del presente Regolamento e di quelle specificatamente sotto indicate:

- le connessioni a internet di carattere non strettamente lavorativo dovranno avvenire fuori orario di lavoro e quindi durante la pausa pranzo ovvero dopo la fine del servizio;
- per quei lavoratori che non sono soggetti a un orario di lavoro prestabilito ci si riferisce, per la determinazione dello stesso, a quello comunque consigliato o comunque a quello risultante da accordi integrativi e/o da successive comunicazioni aziendali;
- nei limiti definiti dalla presente policy aziendale, sono consentite le connessioni per consultazioni varie, la possibilità di effettuare transazioni bancarie nonché di stampare documenti, secondo le regole aziendali di utilizzo delle stampanti multifunzione, di cui all'art. 4.5.2. Del presente regolamento e/o atti purché in misura ragionevole e non indiscriminata e sempre nei limiti di cui al punto primo;
- l'utilizzo della posta elettronica aziendale è consentito sempreché il numero di mail inviate a titolo personale risulti essere non superiore al 5% del complessivo numero di mail inviate dal dipendente nella giornata di riferimento.

Tutte le attività sopra indicate dovranno ispirarsi ai principi di buona fede contrattuale, diligenza e riservatezza e non dovranno superare la soglia della ragionevolezza né procurare danni alle dotazioni aziendali.
L'utilizzatore risponderà di eventuali danni arrecati o di un uso ingiustificatamente esteso delle citate attività sulla base di quanto previsto dal vigente *Codice disciplinare*.

4.3 Prestazione lavorativa svolta al di fuori delle sedi aziendali

Se la prestazione lavorativa avviene al di fuori dei locali aziendali (ad esempio presso il domicilio del lavoratore in caso di telelavoro e anche in luoghi pubblici in caso di smartworking), i sistemi IT Veritas, rendono disponibili due diverse modalità di connessione:

- pubblicazione di un desktop virtuale (VDI), isolato dal contesto del pc locale;
- pubblicazione di specifiche applicazioni.

Modalità differenti di accesso, in caso non siano applicabili quelle standard, saranno oggetto di valutazione specifica da parte dell'ufficio Sistemi informativi.
Il lavoratore, per accedere al sistema di dati aziendale, dovrà provvedere, in caso d'utilizzo di un device personale, a installare uno specifico plugin (Citrix Receiver) e a controllare la presenza di una protezione antivirus aggiornata. Il lavoratore inoltre dovrà:

- porre ogni cura per evitare che ai dati aziendali messi a sua disposizione possano accedere persone non autorizzate presenti nel suo luogo di prestazione fuori sede;
- procedere a bloccare il PC in dotazione in caso di allontanamento dalla sua postazione di lavoro, anche per un intervallo limitato di tempo;
- alla conclusione della prestazione lavorativa giornaliera, archiviare e conservare i documenti eventualmente stampati in cassetti/armadi o altri contenitori chiusi muniti di apposita serratura;
- distruggere documenti/atti non necessari in occasione di una giornata di rientro presso la sede lavorativa.

Veritas metterà a disposizione del lavoratore solo i dati strettamente necessari allo svolgimento della prestazione lavorativa richiesta, limitando le condivisioni delle informazioni o comunque gli accessi alle banche dati aziendali.

4.4 Tracciabilità

Le operazioni di navigazione Internet compiute da tutti gli utenti (dipendenti/collaboratori ecc.), memorizzate dal sistema operativo, vengono conservate per la durata di mesi 6, per le finalità di cui alle disposizioni normative in materia e al fine di essere rese disponibili a fronte di richieste da parte dell'Autorità giudiziaria.
Veritas pertanto:

- archivia e conserva i log della navigazione in internet;
- regolamenta la navigazione delle pagine internet;
- provvede che i firewall installati permettano le navigazioni solo sui siti corrispondenti a categorie previamente autorizzate.

I dati raccolti, considerato che si riferiscono a strumentazioni necessarie a rendere la prestazione lavorativa, potranno essere utilizzati per tutti i fini connessi al rapporto di lavoro, compresi quelli disciplinari.

4.5 Utilizzo dei dispositivi mobili e stampanti

4.5.1 Dispositivi mobili

II telefono cellulare aziendale è uno strumento di lavoro e quindi deve essere utilizzato con cura e diligenza. Eventuali danneggiamenti derivati da caduta accidentale sono considerati eventi che devono intendersi come assolutamente eccezionali. Danneggiamenti ripetuti durante l'anno solare non rientreranno pertanto nel concetto di eccezionalità.

In caso di smarrimento/furto, a partire dal secondo sinistro occorso durante l'anno solare verrà addebitato all'utente l'importo dei canoni di noleggio residui che Veritas è tenuta a risarcire al carrier telefonico (da 50 a 100 euro a evento).

Qualora la richiesta di sostituzione sia derivata da furto o smarrimento della dotazione, l'assegnatario dovrà immediatamente e comunque entro le 24 ore dal furto o dallo smarrimento, e autonomamente provvedere a bloccare la SIM chiamando il numero gratuito TIM 119 da un altro dispositivo e successivamente inoltrare il modulo di richiesta di reintegro su piattaforma Delta9, allegando inoltre la regolare denuncia emessa dalle forze dell'ordine (Polizia, Carabinieri). Nella denuncia dovrà essere specificato chiaramente il bene rubato/smarrito (Telefono, SIM o entrambi) e che questi è di proprietà di Veritas spa. Non sono accettate autocertificazioni.

Nel caso in cui la richiesta non sia corredata dalla denuncia alle autorità non si potrà procedere al ripristino della dotazione e al mantenimento del numero telefonico originario.

I dispositivi mobili devono essere utilizzati esclusivamente con la SIM aziendale abbinata. Non è consentito l'uso del dispositivo aziendale con SIM private o di terzi. È inoltre vietato l'utilizzo della SIM aziendale su dispositivi diversi da quelli consegnati dai Sistemi informativi, salvo eventuali casi particolari obbligatoriamente autorizzati dalla direzione generale.

Le richieste di dotazioni o di sostituzioni per dispositivi mobili devono essere inoltrate tramite portale interno Delta9 allegando il modulo **M TEC 00 "Richiesta servizi di fonia e cellulare aziendale"**. Nel caso di tablet e di attivazione servizio dati l'autorizzazione deve essere riconfermata dal direttore generale.

Prima della sostituzione del telefono/SIM sarà cura dell'utente provvedere a effettuare il backup di tutti i propri contatti telefonici/foto/altro presenti nel telefono riconsegnato (guasto o malfunzionante) sulla propria SIM a su altro dispositivo.

All'atto della sostituzione del telefono guasto a malfunzionante, l'utente dovrà restituire contestualmente il vecchio apparecchio. La mancata riconsegna del vecchio telefono comporta la mancata consegna del nuovo.

In caso di restituzione del telefono cellulare e SIM (cambio mansione, fine servizio ecc.) devono essere restituiti anche i relativi accessori (batteria, caricabatteria ecc.).

La consegna/sostituzione dei dispositivi/SIM è prevista presso l'ufficio TLC nella sede di via Brunacci 28 Marghera il lunedì e giovedì dalle 9.30 alle 11.30.

La sostituzione dell'apparato telefonico avverrà con quanto disponibile, fermo restando le caratteristiche tecniche dell'apparato originario. La sostituzione non implica necessariamente la dotazione di un terminale nuovo, ma la fornitura di un terminale analogo perfettamente funzionante.

Per il servizio di telefonia mobile qualora la SIM dell'assegnatario fosse abilitata al traffico nazionale, è obbligatoria la sottoscrizione di apposita opzione di Dual Billing che consente la distinzione tra le chiamate/sms

aziendali e quelle effettuate a titolo personale mediante un codice di impegno o altra applicazione.
Al di fuori del territorio Nazionale l'utilizzo della SIM aziendale è consentito esclusivamente per esigenze lavorative. Per l'utilizzo del cellulare all'estero deve essere inoltrata richiesta attraverso il portale aziendale interno dal proprio responsabile d'ufficio almeno 2 giorni lavorativi prima della data inizio. La richiesta deve contenere data inizio e data fine abilitazione, il servizio richiesto (telefono, dati) e l'area geografica di utilizzo (Unione Europea, Stati Uniti, Altro).
È concessa la cessione del numero telefonico aziendale a scopo privato esclusivamente al personale in quiescenza con dispositivo direttamente assegnato e in possesso dell'opzione DUAL BILLING. La richiesta deve essere inoltrata con almeno 15 giorni di anticipo rispetto alla data di cessazione del rapporto di lavoro.
Per gli utenti dotati di smartphone, per questione di sicurezza, non è consentita la configurazione di App o account di posta diversi da quelli aziendalmente necessari per la propria attività lavorativa.
L'azienda inoltre provvede a installare sul device un applicativo che consente la protezione dei dati aziendali (account, messaggi, rubrica, altro) in caso di smarrimento/furto del dispositivo. L'applicativo prevede altresì uno "store" aziendale con tutte le Applicazioni (App) che sono autorizzate all'uso sui device di Veritas spa. **Si rammenta che le App che possono essere installate sul device devono avere attinenza con il proprio profilo lavorativo**.
È facoltà dell'utente richiedere all'ufficio Telecomunicazioni e Sistemi di Stampa l'inserimento nello store aziendale di un'applicazione ritenuta necessaria ai fini lavorativi ma non presente. L'ufficio Telecomunicazioni e Sistemi di Stampa effettuerà le doverose verifiche di sicurezza e, se soddisfatte, provvederà al rilascio dell'App per la successiva installazione da parte dell'utente. La richiesta di abilitazione per le nuove App dei dispositivi mobili deve essere inoltrata tramite portale interno Delta9.
Per l'installazione delle App sugli smartphone ogni utente deve disporre obbligatoriamente di un account nominativo per accedere ai servizi dei vari store (Google Play, App Store, Windows Market). L'utente già in possesso di un account potrà utilizzare il proprio, in caso contrario l'ufficio Telecomunicazioni e Sistemi di Stampa provvederà alla creazione di un account *ad hoc* con password temporanea. Sarà poi cura dell'assegnatario modificare la password dell'account e la custodia dei relativi dati di accesso (username e password).
I dati di accesso all'account dello store sono FONDAMENTALI all'atto dell'installazione delle App e nelle pratiche di cambio telefono a seguito di malfunzionamento o altra causa che ne determini la sostituzione. Essendo parametri che identificano l'identità, l'utente è tenuto a conservarli autonomamente con estrema cura. L'ufficio Telecomunicazioni e Sistemi di stampa non custodisce le credenziali personali per l'accesso agli store App.
Si precisa che la connettività DATI presente sui dispositivi smartphone/Tablet/internet Key deve essere utilizzata esclusivamente a fini lavorativi.
Si rammenta che la concessione all'utilizzo privato delle chiamate voce/sms uscenti (Dual Billing) non prevede alcuna deroga su quanto contenuto nel presente regolamento.
Anche i dispositivi mobili sono da ritenersi strumenti necessari allo svolgimento della prestazione lavorativa e pertanto i dati raccolti potranno essere utilizzati secondo quanto previsto dall'art. 4, co. 2 della legge 300/70 così come novellato dal dlgs 151/2015.
Eventuali utilizzi delle dotazioni telefoniche in violazione delle regole aziendali, sono sanzionabili secondo quanto già previsto dal vigente codice disciplinare.

4.5.2 Stampanti

Le stampanti multifunzione aziendali sono anch'esse strumenti di lavoro che devono essere parimenti utilizzate con cura e diligenza, anche al fine di evitare sprechi di carta e/o di toner. Fermo restando che la manualistica per l'utilizzo dei sistemi di stampa è disponibile sul portale aziendale Il Milione, il dipendente pertanto deve:

1. stampare/fotocopiare documenti e atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative;
2. stampare in bianco/nero e fronte/retro al fine di ridurre i costi, laddove possibile;
3. qualora il dipendente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà aver cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati ed evitare di lasciare sul vassoio l'output cartaceo;
4. utilizzare esclusivamente il proprio PIN personale per l'accesso alle stampanti multifunzione. L'uso di credenziali di accesso consentono la stampa soltanto a utenti che effettuano l'autenticazione. Ciò permette al contempo di tracciare e registrare il nominativo, la data e la natura del documento per cui è stata richiesta la riproduzione;
5. utilizzare correttamente i vassoi carta e non modificarne il formato;
6. non introdurre originali sull'alimentatore automatico se con pinzatura metallica;
7. in caso di inceppamento l'utente è tenuto a cercare di ripristinare il funzionamento seguendo le istruzioni a display per quanto possibile. In caso di impossibilità e/o di persistente malfunzionamento contattare direttamente il numero verde dell'assistenza tecnica riportato sull'etichetta posta sul fronte macchina;
8. mantenere pulita la lastra in vetro di esposizione. In caso di necessità provvedere alla pulizia mediante un panno morbido e dell'alcool;
9. sostituire il materiale di consumo (toner e vaschetta recupero) avendo cura di riporre quello di risulta negli appositi contenitori presenti in ciascuna sede aziendale.

In caso di danneggiamento accidentale contattare l'assistenza tecnica della macchina, segnalando immediatamente l'accaduto all'ufficio Sistemi informativi.

È inoltre vietato:

- tentare di manomettere la programmazione/setup dei dispositivi di stampa. In caso di necessità l'utente deve contattare l'ufficio Sistemi informativi.
- eseguire fotocopie di: banconote, vaglia postali, passaporti, francobolli postali, marche da bollo, opere protette da diritto d'autore senza il permesso di chi ne possiede i diritti.

Il trasferimento del dato da stampare dal PC verso la stampante di rete multifunzione è da intendersi **cifrato al fine di** rendere le informazioni non **visibili e non vulnerabili**.

5 Regole comportamentali atte a prevenire crimini informatici

Fermo restando che i Sistemi informativi provvedono all'attivazione di sistemi antivirus e anti spamming su tutti i dispositivi aziendali collegati alla rete Veritas, di seguito vengono descritte le principali regole da osservare per evitare di incorrere in comportamenti illeciti o da cui possano derivare rischi per l'azienda.

Tali regole disciplinano i comportamenti da seguire relativamente ai seguenti aspetti:

- attività di spam;
- diffusione di virus e malware;
- attacchi informatici e accessi abusivi ai sistemi;
- pubblicazione e diffusione di materiale offensivo, molesto o sovversivo;
- violazione del diritto d'autore e del copyright;
- diffusione di materiale pedo-pornografico;
- frodi informatiche e furto d'identità;
- violazione del segreto aziendale;
- trattamento illecito di dati personali e di traffico.

In ogni caso, chiunque abbia in dotazione un PC fisso o portatile, è tenuto a collegarlo alla rete aziendale con il

cavo di rete, con cadenza almeno mensile, per verificare che vengano eseguiti correttamente tutti gli aggiornamenti previsti da remoto.

5.1 Attività di spam

Con il termine spam si indica l'invio di messaggi di posta elettronica a un gran numero di destinatari che non ne abbiano specificatamente fatto richiesta o che non abbiano esplicitamente acconsentito a riceverli.
Obiettivo principale dello spamming è la pubblicità: dalle semplici offerte commerciali, a proposte di vendita di materiale pornografico/pedopornografico, fino a tentativi di truffa veri e propri.

5.1.1 Modalità operative spam

- Non iniziare o partecipare a una catena di corrispondenza ("catene di S. Antonio") né aderire a messaggi di tipo "*hoax*" (burle ricevute via e-mail che fanno leva sulla credulità del ricevente relativamente a storie drammatiche o alla diffusione di presunti virus);
- evitare di diffondere il proprio indirizzo e-mail aziendale attraverso siti, forum, chat, *newsletter* o quanto altro non pertinente all'attività lavorativa;
- non accettare mai l'invito a rimuovere il proprio nominativo da una mail list per evitare di confermare allo spammer la validità dell'indirizzo mail;
- non aprire i messaggi che appaiono palesemente come spam e cancellarli tempestivamente dalla mailbox;
- eliminare tempestivamente gli allegati a messaggi di posta elettronica se il mittente è sconosciuto o in caso di mittente noto il testo della mail è in una lingua differente da quella attesa o è composto da frasi senza senso;
- segnalare allo specifico servizio interno le mail di spam ricevute, secondo le modalità reperibili sull'intranet;
- non disabilitare o inibire il corretto funzionamento del software anti-virus;
- non aprire allegati/link con informazioni non pertinenti con l'attività dell'ufficio.

5.2 Diffusione di virus e malware

Con virus e *malware* si intendono programmi malevoli che possono provocare malfunzionamenti e danni ai sistemi informatici aziendali mettendo a rischio l'integrità, la disponibilità e la riservatezza di dati e applicazioni ivi residenti. Nello specifico, un *malware* appartiene alla categoria dei virus quando si identifica in un programma che si inserisce all'interno di file eseguibili o in aree particolari del sistema, con la capacità di "riprodursi" e di duplicarsi, senza che l'utente ne sia a conoscenza sfruttandone la sua attività. I virus possono essere più o meno dannosi per il sistema operativo che li ospita, ma, in ogni caso, comportano sempre uno spreco di risorse in termini di RAM, CPU e spazio sul disco fisso.

5.2.1 Modalità operative per evitare o limitare danni da virus e malware

- Non installare né utilizzare software che non siano stati regolarmente acquisiti e distribuiti tramite i canali aziendali o comunque non autorizzati dai sistemi informativi;
- non aprire documenti di provenienza incerta;
- eliminare tempestivamente le e-mail di provenienza sconosciuta e/o con contenuto sospetto;
- non eseguire programmi ricevuti come allegati a messaggi di posta elettronica senza preventivamente averli scaricati sulla postazione di lavoro e averli sottoposti a controllo con antivirus;
- non visitare siti di dubbia reputazione né eseguire il download di file eseguibili se non si conosce la fonte di provenienza e se non si è espressamente autorizzati;
- durante la navigazione Web e/o la lettura delle e-mail, diffidare delle URL particolarmente lunghe contenenti sequenze di valori esadecimale e dialog box che propongono l'installazione di plug-in o applicativi vari, anche se firmati in modo digitale, di cui l'autore è ignoto;
- segnalare prontamente la presenza di eventuali virus secondo le modalità reperibili sulla rete intranet.

5.3 Attacchi informatici e accessi abusivi ai sistemi

Per attacchi informatici si intendono eventi che sfruttano le vulnerabilità di un sistema al fine di utilizzare/alterare le informazioni senza averne i privilegi adeguati e/o di compromettere, anche attraverso una ripetizione di sequenze di operazioni lecite, il regolare funzionamento dei sistemi. Sono altresì considerati attacchi informatici quelle azioni volte a ottenere l'accesso a un sistema o a uno specifico oggetto al fine di effettuare su di esso operazioni senza essere in possesso dei privilegi necessari, oppure per scopi diversi da quelli per cui l'accesso è stato autorizzato. L'accesso abusivo infatti consiste nell'introdursi in un sistema informatico o telematico protetto da misure di sicurezza ovvero nel mantenervisi contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

5.3.1 Modalità operative da seguire in caso di attacchi informatici

- Adottare la massima accortezza durante l'utilizzo e la conservazione delle credenziali di autenticazione (nome utente, password, smart card ecc.) di accesso ai sistemi informatici in modo da evitare una possibile perdita di riservatezza;
- provvedere tempestivamente al cambio della password e comunicare al proprio responsabile gerarchico o referente aziendale, anche solo nel caso in cui si abbia un sospetto, la perdita di riservatezza delle credenziali di accesso ai sistemi informatici;
- scegliere una password robusta e difficilmente intuibile da altri, costruendo la stessa sulla base di quanto disposto dalle normative interne (lunghezza minima 8 caratteri, contenente lettere, numeri e caratteri speciali);
- non lasciare incustodita e accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- non lasciare incustoditi documenti contenenti dati riservati e/o informazioni che possono consentire a soggetti terzi di accedere ai sistemi informatici aziendali; in caso di dismissione dei suddetti documenti provvedere tempestivamente alla distruzione degli stessi mediante apposite apparecchiature (ad esempio trita documenti nel caso di documenti in formato cartaceo);
- non accedere né tentare l'accesso a informazioni per i quali non si possiedono i privilegi autorizzativi;
- non utilizzare credenziali dei colleghi, seppure fornite in buona fede, ma richiedere e utilizzare sempre accessi nominativi personali;
- mantenere la corretta configurazione della propria postazione di lavoro non alterando le componenti hardware e software predisposte allo scopo, né installando ulteriori software non autorizzati;
- non installare/collegare sul proprio personal computer mezzi di comunicazione o altre periferiche proprie (ad esempio modem, masterizzatori, smartphone, usb devices);
- non servirsi di strumenti che consentano di restare anonimi sulla rete (ad esempio TOR, proxy);
- non connettere la propria postazione di lavoro a una rete esterna (*wireless*, modem, 4g-lte) salvo quella aziendale, in caso di specifica abilitazione;
- non utilizzare e/o installare software atti a danneggiare o sovraccaricare i sistemi o la rete;
- non utilizzare e/o installare software atti a intercettare, falsificare, alterare il contenuto di documenti informatici (ad esempio programmi di password *recovery, cracking, sniffing, spoofing, serial codes*);
- verificare che sui sistemi di propria competenza vengano regolarmente e tempestivamente applicate le patch software di sicurezza distribuite dai vendors e dai Sistemi informativi tramite "Windows update";
- applicare le regole previste per contrastare la diffusione di virus e *malware*.

5.4 Pubblicazione e divulgazione di materiale offensivo, molesto o sovversivo

Si tratta di fenomeni offensivi e lesivi della dignità umana della libertà individuale e della pubblica morale che spaziano dalle molestie (sessuale, morale, minacce in senso generico o a carattere persecutorio) alla discriminazione razziale ed etnica, religiosa, politica e sessuale. Sono, altresì inclusi quei fenomeni che perseguono scopi contrari all'ordine pubblico, che offendono la religione di stato e/o gli ordinamenti statali.

5.4.1 Modalità operative divulgazione materiale offensivo

Non utilizzare i servizi di rete aziendale quali posta elettronica, internet, intranet per inviare, pubblicare e/o memorizzare materiale dal contenuto:

- offensivo, quali commenti circa l'orientamento religioso, politico, le origini razziali, il colore della pelle e in generale che possa essere lesivo della dignità della persona;
- a sfondo sessuale, pornografico o di natura oltraggiosa;
- offensivo nei confronti degli organi istituzionali dello stato;
- sovversivo contro l'ordine pubblico;
- diffamatorio, calunnioso denigratorio e molesto nei confronti di terzi.

5.5 Violazione del diritto d'autore e del copyright

Con il termine "diritto d'autore" si intende l'insieme dei diritti attribuiti all'autore di un'opera dell'ingegno (musica, libri, film) che riconoscono allo stesso, la facoltà esclusiva di sfruttamento economico e/o la diffusione dell'opera medesima.

Ogni opera dell'ingegno presente su Internet appartiene al proprio autore e non è possibile copiarla modificarla o beneficiarne in alcun modo senza il consenso esplicito dello stesso autore, che ne autorizzi, magari regolamentandolo, l'utilizzo.

La tutela sul diritto d'autore si estende anche alle opere informatizzate, in particolare ai programmi per elaboratore e alle banche dati intese come "raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti e individualmente accessibili grazie a mezzi elettronici o in altro modo".

Pertanto è fatto obbligo di:

- non installare e utilizzare software privi di regolare licenza;
- non scaricare, indebitamente, e/o diffondere video, file musicali e software, giochi o altro materiale protetto da diritto d'autore;
- non sono consentiti la memorizzazione e lo scambio mediante la rete aziendale, di materiale audiovisivo, fotografico, cinematografico, informatico protetto da copyright anche se non effettuato a scopo di lucro;
- non è consentito duplicare, distribuire, adattare e trasformare software regolarmente licenziati da Veritas spa per usi privati e comunque diversi dall'utilizzo consentito per l'attività lavorativa;
- non utilizzare la posta elettronica o le cartelle condivise di rete, per memorizzare o spedire materiale che violi il copyright;
- non utilizzare un'informazione, un testo, un'immagine all'interno dei propri lavori senza citare Esplicitamente la fonte;
- non è consentita la riproduzione, pubblicazione, distribuzione, totale o parziale, di materiale protetto da diritto d'autore;
- non è consentito rimuovere né utilizzare strumenti atti a eludere le misure tecnologiche di protezione del materiale protetto dal diritto d'autore.

5.6 Diffusione di materiale pedo-pornografico

Le fattispecie di reato connesse alla pedo-pornografia on-line riguardano la produzione, divulgazione o diffusione, la commercializzazione, la detenzione e lo scambio di materiale pedo-pornografico intendendo con tale accezione "qualsiasi rappresentazione, con qualsiasi mezzo, di un bambino dedito ad attività sessuali esplicite, concrete o simulate o qualsiasi rappresentazione degli organi sessuali di un bambino a fini soprattutto sessuali" (Convenzione Internazionale sui Diritti dell'Infanzia).
Rientra nella nozione di pornografia infantile anche il concetto di pedo-pornografia virtuale (immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali).

5.6.1 Modalità operative in caso di violazione - diffusione materiale pedo-pornografico

- Non detenere sulle postazioni aziendali e su altri strumenti di archiviazione di massa (ad esempio USB, hard disk, CD-DVD) materiale pedo-pornografico anche virtuale;
- qualora accidentalmente si venisse a conoscenza di materiale illecito di carattere pedo-pornografico, anche virtuale, è divieto assoluto diffondere i contenuti tramite servizi di rete aziendale (internet, intranet e posta elettronica);
- non scambiare, cedere e/o vendere materiale pedo-pornografico anche virtuale utilizzando i servizi di rete aziendali;
- segnalare tempestivamente la presenza di materiale pedopornografico ai Sistemi informativi e alla Direzione Risorse umane e organizzazione di Gruppo.
- effettuare la segnalazione seguendo le modalità indicate nella normativa aziendale di riferimento e sul portale.

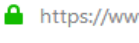
5.7 Frodi informatiche e furto d'identità

La frode informatica viene perpetrata mediante l'accesso, l'alterazione, la cancellazione o soppressione di dati o programmi informatici effettuati al fine di cagionare un danno (economico o materiale) a terzi e un ingiusto profitto (inteso quale vantaggio relativo a interessi morali psicologici o patrimoniali) per se stessi o per altri. Questa si distingue dalla truffa in quanto l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), bensì il sistema informatico.
Il furto dell'identità è un particolare tipo di frode informatica che permette al truffatore di ottenere una serie di vantaggi (economici o materiali) attraverso l'utilizzo improprio dell'identità altrui, avvalendosi di informazioni sensibili carpite alla presunta vittima (n. carta credito, indirizzo, n. di conto corrente, n. telefonico ecc.)

5.7.1 Modalità operative in caso di frodi informatiche

- Non rispondere a messaggi di posta elettronica che richiedono la verifica delle proprie credenziali per l'accesso ai servizi finanziari (di banche o altri istituti finanziari);
- non inserire i propri dati di login cliccando direttamente sui link proposti all'interno di una e-mail, ma digitare l'indirizzo del sito manualmente per essere certi, di non incorrere in siti contraffatti (ad esempio *phishing*, *pharming*);
- non cancellare la sottoscrizione a una mail list di cui non si è certi dell'iscrizione; potrebbe trattarsi di un raggiro da parte di uno spammer per ottenere conferme sulla validità dell'indirizzo e-mail dell'utente;
- utilizzare solo ed esclusivamente le credenziali di accesso assegnate per l'accesso ai sistemi per cui si è autorizzati;
- non scrivere la password su fogli, biglietti od oggetti che vengono lasciati in prossimità del PC (ad esempio sul video, sopra o sotto la tastiera);
- non cedere a terzi credenziali di autenticazione personali (ad esempio nome utente, password, *smartcard*)

di accesso ai sistemi informatici;

- non comunicare la password per telefono o altro mezzo a soggetti che si presentano come colleghi, tecnici o supervisori;
- non aprire mai allegati presenti su e-mail ritenute sospette in quanto è possibile che tali allegati una volta aperti, installino un programma che permettere a soggetti terzi di accedere alle informazioni riservate presenti sulla postazione di lavoro nonché di visualizzare tutto ciò che viene digitato sulla tastiera del computer (ad esempio *keylogging*);
- utilizzare e verificare l'aggiornamento dei programmi (antivirus, browser) installati sulla propria postazione di lavoro;
- verificare prima di accedere sul sito web desiderato che sia stata avviata una sessione protetta (ad esempio accertandosi che l'indirizzo web cominci con https e che il simbolo accanto all'indirizzo sia un "lucchetto chiuso", ad esempio 

);
- non intervenire in modo fraudolento su dati, informazioni o programmi contenuti in un sistema informatico/telematico;
- proteggere i documenti informatici contro tentativi di falsificazione mediante strumenti di firma digitale e crittografia quando previsto;
- non fornire i propri dati personali a società di dubbia reputazione o comunque accettarsi sempre della veridicità del sito web prima di inserire i propri dati sensibili (ad esempio numero carta di credito);
- classificare e gestire correttamente le informazioni aziendali, sotto il profilo della riservatezza, secondo quanto previsto da apposita normativa interna;
- segnalare tempestivamente alla competente struttura aziendale tutti i casi di truffa informatica di cui si viene a conoscenza durante l'espletamento delle proprie mansioni.

6 Provvedimenti

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento costituisce inosservanza delle disposizioni al personale e può essere quindi oggetto di provvedimenti disciplinari ai sensi della vigente normativa contrattuale, nonché nei casi più gravi di azioni civili e/o penali – ove consentite – nei confronti dei trasgressori.

7 Entrata in vigore

Il presente Regolamento entra in vigore a seguito di apposita approvazione da parte del Cda di Veritas spa.

Allegato A

Rif.: Direzione Risorse Umane e Organizzazione

Venezia,

Al Dipendente/Collaboratore

_____

Oggetto: consenso informato
All. "A" al Regolamento per l'Utilizzo del Sistema Informatico
Informativa ex art. 13 Regolamento 2016/679

Il presente documento definisce le condizioni generali di accesso al servizio Internet sfruttando il collegamento alla rete di Veritas spa.

Il collegamento alla rete Internet attraverso l'accesso aziendale può avvenire da un qualsiasi PC (personal computer) di Veritas spa abilitato al servizio, mediante inserimento della propria username e password (logon al sistema). L'attivazione del servizio viene eseguita dall'ufficio Sistemi informativi previa richiesta/autorizzazione da parte del dirigente competente.

Diritti e doveri del dipendente

1. Il dipendente/collaboratore prende atto dell'esistenza del registro dei collegamenti (log) mantenuto da sistema anti-intrusione.
2. Il dipendente/collaboratore prende atto che Veritas spa, adotta tutte le misure tecniche e organizzative necessarie a garantire la riservatezza del registro degli eventi in conformità alle prescrizioni di cui al Regolamento UE 2016/679;
3. Il dipendente/collaboratore prende atto che il registro degli eventi potrà essere esibito su richiesta dell'Autorità Giudiziaria.
4. Il dipendente/collaboratore si impegna, nell'utilizzo del servizio, al rispetto delle vigenti disposizioni normative e di legge in materia.
5. Il dipendente/collaboratore dà atto di essere informato sul contenuto del Regolamento aziendale vigente per l'utilizzo del Sistema informatico e sulle vigenti disposizioni normative e di legge che ne disciplinano l'uso, ivi compresa la possibilità che i dati raccolti rispetto alle strumentazioni assegnate per lo svolgimento della prestazione lavorativa possano essere utilizzati per tutti i fini connessi al rapporto di lavoro, compresi quelli disciplinari ex art. 4, co. 2 legge 300/70.

dott. Andrea Razzini

direttore generale