NapoliServizi

REGOLAMENTO INFORMATICO AZIENDALE

Premessa

La Napoli Servizi S.p.A. intende promuovere l'utilizzo della Rete Informatica e Telematica, di Internet e della Posta Elettronica quali strumenti utili a perseguire le proprie finalità.
La realizzazione e la messa in esercizio dell'infrastruttura di rete aziendale, in grado di erogare servizi centralizzati fruibili anche da sedi remote, introduce pertanto l'obbligo di stabilire alcune regole fondamentali sul corretto utilizzo del sistema informativo, al fine di prevenire l'insorgere di inconvenienti che, anche in buona fede, a vari livelli possono pregiudicarne il regolare funzionamento o addirittura arrecare danni concreti all'azienda sotto il profilo legale, economico, operativo e di immagine.

Il presente documento costituisce così il **"Regolamento Informatico" (RIA)**, che la Napoli Servizi adotta con l'obiettivo di diffondere tra i propri dipendenti la cultura della sicurezza nell'utilizzo degli strumenti informatici, ispirandosi a principi di correttezza e diligenza. Esso, inoltre, si aggiunge ed integra:

- gli altri adempimenti tipici della disciplina della tutela della riservatezza in ottemperanza al d.lgs.vo 196/2003;
- le regole di comportamento indicate nel "Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001" (MOGC) e in special modo al capitolo IV della Parte Speciale VI.

Si precisa che il mancato rispetto delle misure di sicurezza tecnico-strumentali potrebbe comportare non solo effetti sanzionatori dettati dalla normativa in materia di privacy, ma anche una ripercussione di carattere sanzionatorio relativa alla "responsabilità per l'esercizio di attività pericolosa", art. 2050 c.c., nel caso di inadempienze derivanti da violazione delle norme concernenti sia le modalità di trattamento che il danno patrimoniale.

Le indicazioni di seguito riportate hanno quindi un diretto effetto prescrittivo e il carattere di obbligatorietà, con decorrenza dalla data di distribuzione del documento stesso.
La Napoli Servizi porrà in essere azioni di verifica al fine di monitorare l'integrità del proprio sistema informatico e il rispetto delle regole. Poiché la loro violazione, parziale o totale, dovrà ritenersi oggetto di valutazione con conseguenze proporzionate alla gravità degli atti o comportamenti assunti, se ne suggerisce un'attenta lettura, al fine di procedere all'accettazione dei contenuti in modo consapevole mediante sottoscrizione.

1. Entrata in vigore e diffusione del RIA

La prima stesura del regolamento è ufficialmente entrata in vigore dal 20/05/2013, per cui tutte le disposizioni in precedenza adottate in materia devono intendersi abrogate e sostituite da quelle contenute nell'ultima versione del presente documento.

Copia del regolamento, oltre ad essere affisso nella bacheca aziendale, verrà consegnato a ciascun utente del sistema informativo aziendale contestualmente all'affidamento della postazione informatica e/o all'erogazione delle credenziali di accesso, con l'obbligo di controfirmare per ricevuta ed espressa visione la lettera di accompagnamento.

4. Interventi tecnici di manutenzione, sicurezza e salvaguardia del sistema informatico

Il personale incaricato che opera presso la funzione Servizi Informativi della Napoli Servizi è stato autorizzato a compiere interventi, nel sistema informatico aziendale, con le seguenti finalità:

- garantire la sicurezza e la salvaguardia del sistema
- monitoraggio dell'osservanza del presente Regolamento ovvero in caso di riscontro di abusi
- per motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.).

Detti interventi, in considerazione dei divieti enunciati nel presente documento potranno anche comportare l'accesso, in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché la verifica dei siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata o impedimento dell'utente, nelle modalità previste dal d.lgs.vo 196/2003.
L'accesso del personale dei Servizi Informativi alle postazioni di lavoro è limitato al tempo necessario all'espletamento dell'intervento previsto e opportunamente comunicato all'utente (in via preventiva, se possibile, oppure a conclusione dello stesso in caso di particolare urgenza).

Il personale incaricato dei Servizi Informativi ha anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa. Tali interventi vengono effettuati esclusivamente su richiesta dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico. In quest'ultimo caso, e sempre che non si pregiudichi la tempestività ed efficacia dell'intervento, verrà data comunicazione all'utente della necessità dell'intervento stesso.

Al fine di garantire l'integrità del sistema, i Servizi Informativi hanno implementato nell'infrastruttura informatica una serie di strumenti ed impostazioni che in modo proattivo tendono ad impedire del tutto o attenuare significativamente il rischio di abusi e minacce informatiche. I principali strumenti e le configurazioni implementate fanno riferimento a:

- Adozione di software antivirus (in versione enterprise) su tutti i pc e server, con gestione centralizzata di aggiornamenti, avvisi e monitoraggio
- Adozione di software antispam sul server di posta elettronica aziendale
- Protezione della connessione Internet con firewall ad elevato standard di sicurezza
- Implementazione del servizio di Web Content Filtering che consente la navigazione Internet solo su categorie di siti preventivamente abilitate mediante specifiche policy
- Impostazioni dell'ambiente server Microsoft Windows (Active Directory) per la gestione centralizzata dei criteri di utilizzo delle risorse informatiche condivise da parte degli utenti
- Impostazioni dei sistemi operativi client (pc) che, attribuendo agli utenti il ruolo di semplice user, impediscono l'alterazione delle configurazioni di sistema e delle dotazioni software installate

5.2 *Modalità di richiesta e assegnazione delle risorse informatiche*

Per ricevere dai Servizi Informativi risorse informatiche in dotazione, per richiedere l'accesso alla rete e/o per abilitazioni all'utilizzo di servizi applicativi, è necessario attenersi alla procedura denominata "Assistenza e supporto informatico".

I materiali hardware e software forniti verranno consegnati agli utenti destinatari, contestualmente alla firma per ricevuta predisposta su apposito modello che elencherà i beni assegnati.

5.3 *Licenze software*

La dotazione software della postazione informatica comprende programmi e applicativi provvisti di regolare licenza d'uso custodita a cura dei Servizi Informativi. Pertanto ogni software estraneo a quelli forniti in dotazione è da considerarsi privo di tale requisito e assimilabile a software "pirata" con conseguenze legali direttamente riconducibili all'utente che lo ha installato.
È opportuno precisare che anche licenze di tipo Freeware o Shareware, se valide per un uso non commerciale del prodotto, non sono idonee ad una installazione in ambito aziendale.

5.4 *Protezione antivirus*

Il sistema informatico aziendale è protetto da software antivirus e antispam aggiornati quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacchi informatici mediante virus o mediante ogni altro software pericoloso.
Nel caso i software antivirus/antispam rilevino la presenza di virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al personale dei Servizi Informativi.

6. Credenziali

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale dei Servizi Informativi, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

Ad ogni utente vengono assegnate un set di credenziali costituito da *nomeutente* e *password*, da utilizzare nelle fasi di autenticazione per l'accesso al sistema informativo aziendale, ai servizi e agli applicativi centralizzati. Per alcuni specifici applicativi potrà essere necessario fornire all'utente ulteriori set di credenziali.

6.1 *Gestione delle credenziali*

L'utente è tenuto a conservare nella massima segretezza i propri dati di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.
Per nessun motivo deve essere consentito ad altri l'utilizzo delle proprie credenziali. Qualsiasi accesso alla rete ed ai sistemi, anche occasionale, deve prevedere l'utilizzo di credenziali personali rilasciate dall'Amministratore di sistema.

7.1 *Profili utente*

Il processo di autenticazione per l'accesso alla rete avviene da ciascuna postazione mediante l'inserimento delle proprie credenziali, a cui corrisponde un profilo utente univoco che fornisce le autorizzazioni necessarie e il grado di operatività sugli applicativi e sulle risorse condivise, basato su indicazioni fornite dai rispettivi responsabili di funzione o dei vertici aziendali.

7.2 *Cartelle di lavoro*

Sui server centralizzati vengono messe a disposizione, per ogni settore aziendale, delle cartelle (directory) ad uso esclusivo o condiviso per l'accesso e la memorizzazione di quei dati che contribuiscono a definire il patrimonio informativo digitale, oggetto di backup periodico al fine di preservarne la disponibilità e l'integrità. La struttura di tali cartelle è predisposta dall'Amministratore di sistema (a cui è sempre garantito l'accesso ai dati per la corretta gestione e manutenzione) secondo lo schema organizzativo aziendale o in base a specifiche richieste dei responsabili di funzione/area, e a cui corrispondono autorizzazioni specifiche riconducibili al profilo utente sopra descritto.

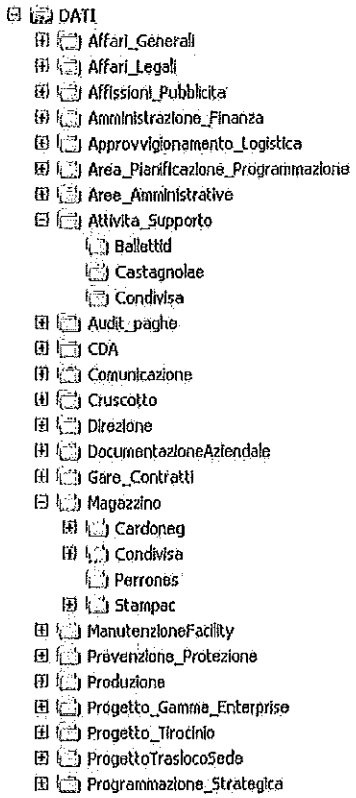

Fig. 1 Esempio di struttura delle cartelle di lavoro

Le cartelle di lavoro denominate "condivisa" (all'interno di ogni settore es.: Affari generali, Amministrazione e finanza ecc.) sono accessibili dai componenti dello specifico settore aziendale e da soggetti che, pur non appartenendovi, hanno ricevuto la necessaria autorizzazione dal corrispondente responsabile di funzione/area.
Le cartelle personali (responsabile, dipendente ecc.) sono invece di tipo individuale, ovvero accessibili solo dal titolare.

In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi/cassetti chiusi.

E' vietato l'utilizzo di supporti rimovibili personali.

I supporti rimovibili, prima di essere utilizzati, devono essere sottoposti obbligatoriamente a controllo antivirus.

9. Connessione e navigazione Internet

Sia per l'utilizzo come strumento di lavoro che per consentire la connessione alla rete aziendale da sedi remote, è prevista per alcune postazioni di lavoro l'abilitazione alla navigazione in Internet. Al fine di limitare il più possibile i rischi derivanti da tale abilitazione, è necessario adottare da parte degli utenti le prescrizioni di seguito riportate:

1. **non modificare in alcun modo le impostazioni di rete e di accesso remoto** del pc. In caso di problemi di connessione richiedere sempre l'intervento degli assistenti informatici;
2. **non utilizzare altri dispositivi di connettività (es.: cellulare) per effettuare connessioni alla rete internet a meno che non si disponga di un dispositivo fornito dall'azienda;**
3. **accedere esclusivamente a siti Internet che presentino adeguate garanzie in termini di attendibilità e contenuti sicuri;**
4. **non accedere a siti i cui contenuti non siano di interesse per l'attività lavorativa** e alle mansioni affidate;
5. **non modificare le impostazioni del browser Internet Explorer,** anche se tali modifiche vengono suggerite dai siti per una corretta fruizione dei contenuti, senza averne preliminarmente verificato l'attendibilità (siti istituzionali, agenzie di stampa ecc.) Nei casi dubbi, qualora venga richiesta la modifica di dette impostazioni (cookies, applet Java, script ActiveX ecc.) richiedere il supporto all'Amministratore di sistema per le necessarie verifiche di sicurezza e poi procedere all'eventuale attivazione;
6. **non attivare alcuna funzionalità di memorizzazione delle password e/o di compilazione automatica dei moduli;**
7. **non scaricare (download) files, documenti o applicazioni protetti da copyright e comunque non attinenti la propria attività aziendale.** Qualora necessario, richiedere il download da Internet all'Amministratore di sistema, che provvederà ad effettuare le necessarie verifiche di sicurezza e di compatibilità del software con il sistema informativo aziendale;
8. **qualsiasi file o software scaricato deve essere verificato con l'antivirus installato sulla postazione;**
9. **non alterare le funzionalità che prevedano l'automatico aggiornamento dei componenti software presenti sulla propria postazione (es.: Windows Update),** al fine di non comprometterne il regolare funzionamento.
10. **non utilizzare il browser o altri programmi per conversazioni in chat line, forum o collegamenti con web cam** se non in circostanze strettamente professionali;
11. **non attivare funzionalità di amministrazione remota della postazione,** se non esplicitamente richiesto dall'Amministratore di sistema o dagli assistenti informatici;

3. **non è consentito inviare tramite e-mail informazioni e/o allegati di particolare rilevanza strategica per l'azienda**, poiché non è possibile garantire la certezza di identità del destinatario e le finalità di utilizzo di tali informazioni;
4. **non è consentita l'iscrizione a mailing list non professionali e l'inoltro di messaggi relativi a "catene di S.Antonio" e simili;**
5. **è vietata l'apertura e/o la memorizzazione di file allegati ai messaggi di posta elettronica provenienti da mittenti sconosciuti o di dubbia identità**, a causa dell'elevata diffusione di minacce alla sicurezza del sistema informativo costituite da virus, spyware, trojan, adware ecc;
6. **per i messaggi provenienti da mittenti attendibili, l'apertura e/o memorizzazione di file allegati deve essere sempre preceduta dalla scansione con il software antivirus residente sulla postazione informatica**, al fine di scongiurarne la pericolosità derivante da un'inconsapevole presenza di virus sulla postazione del mittente;
7. **utilizzare sempre i formati compressi (es.: zip, rar) per ridurre le dimensioni dei file allegati ai messaggi di posta inviati;**
8. **in ogni caso, tenere conto che la dimensione massima degli allegati è pari a 10 Mb.** Qualora necessario, inviare più messaggi contenenti allegati di dimensioni inferiori alla massima consentita.

Per quanto attiene agli aspetti formali è opportuno tenere conto anche delle seguenti indicazioni:

1. scrivere sempre l'oggetto del messaggio evitando di utilizzare oggetti di altre email non rispondenti al contenuto che si intende comunicare
2. firmare il messaggio soprattutto nei casi di utilizzo della casella di posta di settore, specificando il proprio ruolo rispetto all'organizzazione ufficiale (fare riferimento al proprio ordine di servizio per l'utilizzo dei termini: responsabile, supervisore, addetto etc)
3. il modello di firma standard da utilizzare è disponibile nell'area condivisa sui server \\datins\dati\Transito\MODELLI DOCUMENTI AZIENDALI (file firma-email.dot),
4. non utilizzare template o elementi grafici personalizzati
5. il font da utilizzare è: Garamond – dimensione 11
6. fare attenzione all'uso dello stile dei caratteri usando il grassetto/sottolineato per evidenziare solo i punti salienti del messaggio
7. nelle risposte/inoltri seguire il principio della "piramide rovesciata" – il testo che si sta redigendo va collocato all'inizio del messaggio.

11. Utilizzo di fax, stampanti e fotocopiatrici aziendali

Al fine di perseguire l'obiettivo di progressiva dematerializzazione dei documenti ed archivi cartacei e il relativo contenimento dei costi, corre l'obbligo di limitare il più possibile le attività di stampa, prediligendo ove possibile la conservazione e il trasferimento dei documenti in formato elettronico.

In ogni caso si devono preferire, laddove non sussistano requisiti di riservatezza o problemi di qualità/formato, le stampanti di rete di tipo dipartimentale che hanno costi di esercizio inferiori rispetto ad altri dispositivi personali. Detti dispositivi sono stati programmati per eseguire le stampe in modalità riservata dalle postazioni di lavoro in modo che possano essere ritirate solo dall'utente che ha eseguito il lavoro.

senza alterare i logo e le impostazioni standard, adattandoli alle proprie esigenze di stampa A4/A3 – orientamento orizzontale/verticale

- Nel nome file di ogni documento (Word, Excel etc) deve essere indicato: l'ufficio, il titolo del documento e la versione separati da un trattino (ad es. AFC-Budget2015-Ver.1.0.doc)
- Ogni documento di tipo relazione/progetto deve riportare nel piè di pagina:
  - a destra i numeri di pagina nel formato "pag. 1 di 2"
  - a sinistra: l'ufficio, il titolo del documento, la data e la versione (vedasi il piè di pagina del presente documento)
- Per le lettere prevedere solo il numero di pagina a destra, specificando, nel caso venga richiesto dal proprio responsabile/dirigente, l'apposizione a sinistra della propria sigla personale che possa ricondurre successivamente all'autore
- Per ogni revisione dello stesso documento deve essere incrementata la versione (anche nel nome file) e aggiornata la data
- Utilizzare come testo standard (ad es. per il corpo di una lettera) il font Garamond corpo 11
- Utilizzare i font standard presenti in Word per definire i Titoli (H1, H2, etc) e Sottotitoli
- Utilizzare l'interlinea e spaziatura standard prevista in Word
- Utilizzare i punti elenchi e punti numerati standard presenti in Word
- Utilizzare la funzionalità di Word per costruire Sommari e Indici
- Formattare le tabelle con i font standard suddetti e ponendo i titoli delle colonne in maiuscolo. Utilizzare nei limiti del possibile sfondi in sfumature di grigio per le righe/colonne
- Assicurarsi che il documento proponga margini coerenti e dimensioni delle tabelle uniformi, a meno che non sia necessario diversamente.

Inoltre si tenga conto che:

- A causa dell'eterogeneità delle versioni di Office presenti in azienda, se possibile è opportuno prediligere dei formati file con supporto delle versioni meno recenti (es. Office 2003)
- I documenti possono essere distribuiti in formato Office (Word, Excel etc) o in formato di file salvato come Acrobat (.pdf), che diversamente dai pdf scansiti (che sono delle immagini) ne consentono ancora la gestione dei contenuti (es. ricerca e copia di testo).

13. Rapporti con parti terze alla Napoli Servizi (fornitori, collaboratori, ecc..)"

I Partner, i consulenti, i fornitori e parti terze alla Napoli Servizi, devono impegnarsi a rispettare gli obblighi di legge in tema di reati informatici. A tal uopo, i predetti soggetti sono, altresì, tenuti all'osservanza delle clausole inserite nei relativi contratti dagli stessi sottoscritti, così come previsto dal/i Regolamento/i aziendale/i di riferimento.

14. Non osservanza del RIA

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto e/o la violazione delle regole ivi contenute sono perseguibili con provvedimenti disciplinari e risarcitori, nonché con le azioni civili e penali consentite.