artaabruzzo
agenzia regionale per la tutela dell'ambiente
Direzione Generale

Sistema Nazionale per la Protezione dell'Ambiente

Policy sulla sicurezza informatica

Indice generale

Direzione Centrale – Viale G. Marconi, 178 – 65127 Pescara
Tel.: 085/450021 Fax: 085/4500201 E– mail: PEC:
Cod. Fisc. 91059790682 – P. I.V.A. 01599980685

Premessa

La progressiva diffusione delle nuove tecnologie ICT ed in particolare l'utilizzo della posta elettronica ed il libero accesso alla rete Internet, espone l'ARTA Abruzzo e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura tecnica e patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (diritto d'autore, privacy, ecc.), creando evidenti problemi alla sicurezza ed all'immagine dell'Agenzia stessa.

La Policy sulla Sicurezza Informatica è quel documento nel quale sono contenute tutte le disposizioni, comportamenti e misure organizzative richieste ai dipendenti e/o collaboratori aziendali per contrastare i rischi informatici. Tale documento è da consegnare al momento dell'assunzione di ogni dipendente e da re-inviare ogni anno, a cura del responsabile del trattamento dei dati, tramite email con i necessari aggiornamenti e da far firmare ai consulenti o collaboratori che accedono alla rete aziendale.

Premesso che l'utilizzo delle risorse informatiche e telematiche messe a disposizione da Arta Abruzzo deve sempre ispirarsi al principio della diligenza e correttezza, con la presente Policy sulla sicurezza informatica s'intende contribuire alla massima diffusione della cultura della sicurezza in Agenzia, evitando che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza dei sistemi informatici/informativi e nel trattamento dei dati.

Il documento ha lo scopo di ottenere:

- Riservatezza: prevenzione contro l'accesso non autorizzato alle informazioni
- Integrità: le informazioni non devono essere alterabili da incidenti o abusi
- Disponibilità dei dati: il sistema deve essere protetto da interruzioni impreviste

Il mancato rispetto di quanto previsto nel presente documento potrebbe comportare dei seri rischi sulla sicurezza dell'intero sistema, e, pertanto, comportare sanzioni a carico dell'utente.

1. Utilizzo del personal computer

1.1 Il Personal Computer affidato all'utente/servizio è uno strumento di lavoro e deve essere custodito con cura adottando ogni precauzione per evitare ogni possibile forma di danneggiamento. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e soprattutto, minacce alla sicurezza. Il PC dato in affidamento all'utente/servizio permette l'accesso alla rete intranet dell'ARTA Abruzzo ed alla rete internet solo previo inserimento nel dominio aziendale artaabruzzo.local.

1.2 Gli Amministratori di Sistema, individuati con apposito provvedimento, sono autorizzati a compiere interventi nel sistema informatico aziendale diretti a garantire la manutenzione, la sicurezza e la salvaguardia del sistema stesso (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Pur rispettando tutti i criteri di riservatezza, detti interventi potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché al monitoraggio 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'Agenzia, si applica anche in caso di assenza prolungata od impedimento dell'utente su richiesta da parte della Direzione Aziendale o qualora fosse necessario intervenire per la sicurezza dell'intero sistema. Gli Amministratori di Sistema possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

1.3 Gli Amministratori di Sistema hanno la facoltà di collegarsi e visualizzare da remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. A tale scopo sarà possibile installare sui PC client appositi software (agent), normalmente in commercio, per la rilevazione automatica della configurazione hardware e software, che tenga traccia delle modifiche effettuate e della versione dei software installati.

In ogni caso l'intervento da remoto verrà effettuato, dagli Amministratori di Sistema, esclusivamente su chiamata 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 necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

1.4 Gli aggiornamenti del software e dei driver necessari al buon funzionamento della postazione di lavoro saranno effettuati direttamente degli Amministratori di Sistema che provvederanno all'aggiornamento automatico per ciò che attiene la protezione antivirus ed il sistema operativo, per i PC collegati alla rete aziendale, ed interverranno dietro segnalazione dell'utente per ogni ulteriore aggiornamento necessario. Nel caso di PC non collegati alla rete sarà cura dell'utente provvedere all'aggiornamento del sistema operativo e del software antivirus.

1.5 Le stazioni di lavoro vengono predisposte e configurate dagli Amministratori di Sistema per le esigenze dell'utente finale. Nessun utilizzatore del PC è autorizzato a far parte del gruppo "*Administrators*" della macchina per cui non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, né procedere all'installazione di nuovi software, né alla modifica dei software esistenti. Tutte queste operazioni sono di esclusiva competenza degli Amministratori di Sistema.

1.6 L'accesso ad ogni PC avviene tramite la password di accesso al dominio; sarà cura dell'utente utilizzatore avere la massima diligenza e segretezza nel custodire le credenziali di accesso al proprio PC. Le regole impostate a livello di dominio impongono all'utente il cambio della password ogni 6 mesi.

1.7 E' fatto assoluto divieto all'utente di intervenire in qualunque modo sull'hardware in dotazione. In caso di malfunzionamento delle apparecchiature assegnate, l'utente si impegna a darne tempestiva segnalazione agli Amministratori di Sistema.

1.8 Ogni utente deve prestare la massima attenzione nell'utilizzo di memorie di massa esterne, limitandone l'utilizzo, conservandole in luoghi sicuri e avvertendo immediatamente gli Amministratori di Sistema nel caso in cui siano rilevati virus ed adottando quanto previsto all'art.9 del presente documento relativo alle procedure di protezione antivirus.

1.9 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici, in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. Anche in caso di assenza momentanea dalla propria postazione lavorativa, evitare di lasciare libero accesso ai propri dispositivi effettuando, ad esempio, la disconnessione del proprio account onde evitare che si verifichi un utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

2. Utilizzo della rete

2.1 La rete dell'ARTA Abruzzo si basa sul protocollo TCP/IP. Tutte le apparecchiature connesse alla Rete sono configurate per ricevere l'indirizzo IP dinamicamente dal server DHCP oppure con un IP assegnato staticamente a seconda della tipologia di apparecchiatura.

2.2 E' assolutamente vietato connettere alla rete delle macchine configurate con indirizzo IP statico, assegnato direttamente dall'utente, senza una preventiva autorizzazione degli Amministratori di Sistema. Introdurre una macchina con un IP duplicato potrebbe causare un conflitto con l'indirizzo di un server oppure di un altro dispositivo della rete stessa e causare gravi malfunzionamenti alla rete.

2.3 Non è possibile collegare alla rete aziendale qualsiasi dispositivo (pc, pc portatili, tablet, smartphone, router UMTS, bridge, modem, impianti wireless, ecc.) che non sia stato preventivamente autorizzato dal Dirigente della Sezione "Qualità delle Prestazioni, Controllo di Gestione, Performance, Digitalizzazione e Innovazione Tecnologica". Analogamente non è ammesso l'utilizzo non autorizzato di dispositivi per lo sdoppiamento di punti rete (mini switch).

2.4 E' fatto assoluto divieto di configurare servizi già messi a disposizione in modo centralizzato, quali ad esempio, e non solo, DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol), NTP (Network Time Protocol), mailing, accesso remoto, proxy server.

2.5 E' fatto assoluto divieto all'utente di intercettare ed analizzare i pacchetti sulla rete aziendale, utilizzando analizzatori di rete sia software che hardware; l'utilizzo di tali strumenti è strettamente riservato agli Amministratori di Sistema al fine di monitorare le prestazioni della rete aziendale. Nel caso si riscontrasse la presenza di Pc che generano traffico anomalo o che potrebbero far diminuire le prestazioni dell'intero sistema, sarà facoltà degli Amministratori di Sistema procedere al blocco, se necessario, dell'attività di rete del PC.

2.6 L'utilizzo di reti Wireless (rete senza fili, ad onde radio) deve essere autorizzato dalla Sezione "Qualità delle Prestazioni, Controllo di Gestione, Performance, Digitalizzazione e Innovazione Tecnologica" e, nel caso di installazione nelle vicinanze degli strumenti di laboratorio, comunicato alla Sezione Fisica Ambientale che dovrà valutare la compatibilità con le apparecchiature esistenti.

2.7 Le cartelle utenti, o cartelle dei Distretti presenti nei server dell'Agenzia 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 controllo, amministrazione e backup da parte degli Amministratori di Sistema.
Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. dischi fissi interni o esterni al PC) non sono soggetti a salvataggio da parte degli Amministratori di Sistema. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente; si riporta all'art. 8 "Backup e Pulizia", del presente documento.

3. Gestione delle password

3.1 A tutti i dipendenti ed i collaboratori dell'Agenzia viene attivato un account per l'accesso alla rete aziendale nel dominio @artaabruzzo.local e una casella di posta elettronica nel dominio @artaabruzzo.it.
3.2 Le credenziali di autenticazione per l'accesso alla rete e per l'utilizzo del servizio di Posta Elettronica vengono assegnate dagli Amministratori di Sistema., previa formale richiesta, "RICHIESTA DI CONCESSIONE/REVOCA UTILIZZO RETE INTERNET/INTRANET E SERVIZIO DI POSTA ELETTRONICA", sottoscritta dal Dirigente Responsabile della struttura presso la quale l'utente opera, o dovrà operare.
Nel caso di collaboratori a progetto e coordinati e continuativi, stagisti, etc. la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal Dirigente Responsabile della struttura con la quale il collaboratore si coordina nell'espletamento del proprio incarico.
Nell'eventualità il dipendente/collaboratore/stagista cessi o abbia cessato il rapporto con l'Agenzia sarà cura del Responsabile dell'Ufficio di appartenenza dare tempestiva comunicazione agli Amministratori di Sistema, al fine di evitare un possibile uso illecito dei servizi forniti e delle credenziali di autenticazione.
3.3 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (userid) formato dall'iniziale del nome, da un punto e dal cognome (n.cognome), associato ad una parola chiave (password) riservata che dovrà venir custodita dall'utente con la massima diligenza e segretezza e non divulgata.
Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all'utente titolare del codice userid, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi. Non sono ammissibili codici di accesso anonimi.

3.4 La parola chiave, formata da lettere (maiuscole o minuscole), numeri e caratteri speciali, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

3.5 È necessario procedere alla modifica della parola chiave a cura dell'utente, al primo utilizzo e, successivamente, almeno ogni sei mesi (tre mesi nel caso si trattino dati personali particolari). La password deve essere immediatamente modificata, nel caso si sospetti che la stessa sia stata conosciuta da altri ed abbia, quindi, perso la segretezza.

3.6 Qualora la parola chiave fosse stata dimenticata, si procederà alla sua sostituzione d'intesa con gli Amministratori di Sistema che provvederanno, in seguito a segnalazione dell'utente, a far recapitare all'interessato le nuove credenziali di autenticazione; resta inteso che sarà cura dell'utente modificare la password al primo accesso.

3.7 Ogni dipendente dovrà essere dotato di una casella di posta istituzionale che verrà utilizzata per un più rapido scambio delle comunicazioni interne e che dovrà essere consultata con frequenza giornaliera. Sarà cura del Dirigente verificare l'esistenza di tale casella e, in caso negativo, farne richiesta alla Sezione "Qualità delle Prestazioni, Controllo di Gestione, Performance, Digitalizzazione e Innovazione Tecnologica" .

3.8 L'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: 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. A tale scopo si ritiene indispensabile, ove il Sistema Operativo lo permetta, l'utilizzo di sistemi di blocco della tastiera con password.

4. Utilizzo di PC portatili

4.1 L'utente è responsabile del dispositivo portatile (pc, tablet o smartphone) assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

4.2 Ai dispositivi portatili si applicano le regole di utilizzo previste dal presente documento per l'uso dei Personal Computer. Particolare attenzione è rivolta nel caso di un utilizzo temporaneo del PC portatile assegnato, per ciò che attiene alla rimozione da parte dell'utente utilizzatore di eventuali file elaborati ed utilizzati, prima della riconsegna.

4.3 I dispositivi portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

4.4 Tali disposizioni si applicano anche nei confronti di incaricati esterni quali consulenti, collaboratori, etc.

4.5 Eventuali configurazioni di connessione alla rete LAN, dirette verso la rete aziendale o verso la rete esterna, possono essere attivate esclusivamente seguendo le medesime procedure previste per l'accesso alla rete intranet/internet nel successivo art.6.

E' vietato utilizzare all'interno delle sedi dell'Agenzia delle connessioni di tipo Accesso Remoto, e quindi eventuali modem (hotspot personali), se non espressamente autorizzati dal Dirigente della Sezione "Qualità delle Prestazioni, Controllo di Gestione, Performance, Digitalizzazione e Innovazione Tecnologica". E' prevista la connessione alla rete internet e l'accesso alla rete intranet dietro apposita configurazione del PC da parte degli Amministratori di Sistema.

4.6 Nel caso in cui nel PC portatile vengano memorizzati dati personali, il file system del disco fisso deve essere crittografato. Il Dirigente Responsabile del servizio a cui è assegnato il pc portatile dovrà fare una richiesta in tal senso agli Amministratori di Sistema che provvederanno all'operazione di crittografia del file system.

4.7 Non è consentito l'utilizzo di dispositivi portatili personali se non in caso eccezionale e comunque dietro richiesta al Dirigente della Sezione "Qualità delle Prestazioni, Controllo di Gestione, Performance, Digitalizzazione e Innovazione Tecnologica" .

5. Utilizzo della PEO e della PEC

5.1 Ad ogni Distretto e alla Sede Centrale viene assegnata una casella di posta elettronica certificata utilizzando il seguente formato: dist.xxxxx@pec.artaabruzzo.it o sede.centrale@pec.artaabruzzo.it

5.2 La casella è nominativa ed è associata al Direttore del Distretto o al Direttore Generale

5.3 L'Area Amministrativa deve informare gli Amministratori di Sistema di ogni variazione dei Direttori al fine di procedere ad una corretta assegnazione delle caselle PEC istituzionali.

5.4 Ogni casella PEC deve essere associata al protocollo del Distretto o Area corrispondente.

5.5 La PEC deve essere utilizzata esecutivamente per comunicazioni ufficiali che richiedono la conferma insindacabile dell'avvenuta ricezione della comunicazione inviata.

5.6 Per lo svolgimento delle mansioni lavorative, viene attribuita, a tutti i dipendenti una casella di posta elettronica aziendale ordinaria (PEO). Si raccomanda di utilizzare l'email esclusivamente per finalità legate all'attività lavorativa.

5.7 Le caselle di posta sono nominative e vengono assegnate utilizzando il seguente formato: n.cognome@artaabruzzo.it

Inoltre, per esigenze organizzative del lavoro, ad ogni Distretto ed alla Sede Centrale viene assegnata una casella di posta istituzionali del tipo:.

dist.xxxxx@artaabruzzo.it

info@artaabruzzo.it

Detta casella di posta istituzionale verrà utilizzata per un più rapido scambio delle comunicazioni interne e dovrà essere consultata con frequenza giornaliera. Sarà cura del Direttore del Distretto o dell'Area verificare l'esistenza di tale casella e, in caso negativo, farne richiesta alla Sezione "Qualità delle Prestazioni, Controllo di Gestione, Performance, Digitalizzazione e Innovazione Tecnologica". In tale richiesta dovranno essere elencati i nominativi delle persona autorizzate all'utilizzo della casella di posta istituzionale.

E' previsto, come standard per ogni casella di posta, un dimensionamento massimo pari a 10 GB; qualora fosse necessario un dimensionamento maggiore bisogna farne richiesta alla Sezione "Qualità delle Prestazioni, Controllo di Gestione, Performance, Digitalizzazione e Innovazione Tecnologica"

5.8 L'accesso alla casella di posta elettronica è possibile attraverso la Home Page del sito aziendale (www.artaabruzzo.it) utilizzando le apposite credenziali di autenticazione fornite come indicato in precedenza; sarà possibile, cliccando sulla voce "Web mail", entrare nell'area riservata e da qui accedere alla propria casella di posta. L'accesso diretto può essere effettuato dalla pagina https://webmail.artaabruzzo.it.

In questo modo l'utente potrà consultare la propria casella direttamente via web, collegandosi al Server; tutto ciò offre all'utente la possibilità di accedere alla propria posta ovunque si trovi.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti che alla lunga saturano lo spazio disponibile. Si ricorda a tal fine che sarà necessario eliminare anche i messaggi contenenti allegati di grandi dimensioni presenti nelle cartelle *Posta Inviata, Posta Eliminata*; si raccomanda inoltre di procedere all'eliminazione

definitiva dei messaggi che vengono spostati nella cartella *Posta Eliminata* utilizzando la voce *Svuota Cestino*.

5.9 La casella di posta, assegnata dall'Agenzia all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse pertanto:

- E' vietato utilizzare l'indirizzo e caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.
- E' vietato utilizzare la login/password di un altro utente per accedere in sua assenza alla sua posta elettronica.
- È vietato inviare catene telematiche (le cosiddette "catene di Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo, non si devono in alcun caso attivare gli allegati di tali messaggi.

5.10 Nel caso di prolungata assenza dell'utente e in caso di urgenza, qualora si renda necessario per esigenze lavorative accedere alla posta elettronica o alla postazione di lavoro dell'utente, a giudizio del Responsabile della Sezione, quest'ultimo potrà richiedere l'abilitazione alla Sezione "Qualità delle Prestazioni, Controllo di Gestione, Performance, Digitalizzazione e Innovazione Tecnologica"

5.11 Si raccomanda:

- di prestare attenzione alla dimensione degli allegati che, di norma, non devono mai superare i 20 MB.
- di utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.7z)
- nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.
- di dare immediata segnalazione agli Amministratori di Sistema nel caso si riscontrassero dei casi di phishing (è un tipo di frode ideato allo scopo di rubare importanti dati personali dell'utente, ad esempio numeri di carta di credito, password, dati relativi al proprio conto e così via. Gli autori delle frodi sono in grado di inviare milioni di messaggi di posta elettronica fraudolenti che, in apparenza, sembrano provenire da siti Web sicuri, come la propria banca o la società di emissione della carta di credito, che richiedono di fornire informazioni riservate).

5.12 L’iscrizione a "mailing list" esterne è concessa solo per motivi professionali. Prima di iscriversi occorre verificare in anticipo se il sito è affidabile.

5.13 E' obbligatorio controllare i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti o non affidabili).

5.14 E’ fatto divieto di inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

5.15 Il sistema informatico aziendale utilizza un sistema antispam/antivirus che potrebbe comportare il blocco, in entrata o in uscita, di eventuali messaggi ritenuti nocivi, indesiderabili o potenzialmente infetti. Pertanto è buona norma, nel caso di messaggi importanti, utilizzare la posta elettronica certificata.

6. Utilizzo della rete internet

6.1 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.

6.2 Non possono essere utilizzati hotspot personali per il collegamento alla rete.

6.3 L’accesso alla rete Internet è da intendersi quale “strumento di lavoro”. In tal senso, l’utente non potrà utilizzare internet per:

- l’upload o il download di software gratuiti (freeware) e shareware, nonché l’utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all’attività lavorativa;
- il download, da siti non istituzionali o comunque non ritenuti affidabili, di file eseguibili potenzialmente dannosi o infetti. Qualora, per motivi di lavoro, fosse necessario scaricare uno di questi file da un sito non accessibile, la Sezione "Qualità delle Prestazioni, Controllo di Gestione, Performance, Digitalizzazione e Innovazione Tecnologica" potrà autorizzarne, anche solo temporaneamente, il download previa richiesta sottoscritta dal Dirigente responsabile dell’Ufficio;
- il download di file del tipo MP3, AVI, MPG, Quicktime e/o altri tipi di file o programmi per la fruizione di contenuto audio/video non legati ad un uso d’ufficio;

- ricerche e/o consultazioni di siti il cui contenuto informativo appaia osceno, offensivo alla morale nonché alla pubblica decenza, a contenuto discriminatorio di taluni o razzista, a sfondo politico e/o religioso;
- trasferire sulla stazione dell'utente programmi e/o file di dati relativi a progetti o obiettivi estranei all'attività lavorativa dell'utente o per finalità personali;
- ricerche e/o consultazioni palesemente incompatibili con i fini istituzionali dell'Agenzia;
- 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 dal Dirigente Responsabile del proprio Ufficio 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'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;

È vietato l'uso del servizio nei casi che configurano un più grave reato:

- Diffusione di virus, cavalli di troia o altri programmi, la cui azione consista nel sabotaggio, distruzione o alterazione del contenuto informativo delle stazioni degli altri utenti, degli elaboratori aziendali e dei dati in essi contenuti, anche qualora l'obiettivo sia all'esterno della rete aziendale;
- Per attività di furto di dati di altri utenti, organismi e/o aziende;
- Per attività di hackeraggio e pirateria informatica in generale.

6.4 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Agenzia adotta uno specifico sistema di blocco o filtro automatico (sistema di Web Filtering) che previene determinate operazioni quali il file-sharing o l'accesso a determinati siti inseriti in una lista di siti non autorizzati.

7. Utilizzo del software di gestione documentale

7.1 Il software di gestione documentale e protocollo informatico deve essere utilizzato nel rispetto delle politiche di sicurezza generali descritte nel presente documento. Le credenziali di accesso al sistema sono quelle del dominio.

7.2 Per ogni dipendente il Dirigente della struttura deve indicare agli Amministratori di Sistema l'Ufficio di appartenenza tenendo presente che i documenti assegnati all'Ufficio saranno visibili a tutti gli utenti appartenenti a tale Ufficio.

7.3 In fase di assegnazione di un documento contenente dati personali deve essere applicato il principio di minimizzazione: il documento deve essere assegnato al minor numero di persone possibile se non addirittura alla sola persona interessata.

7.4 Nel caso in cui venga inserito nel gestore documentale un documento contenente dati personali particolari (origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, ecc...) deve essere utilizzata la funzione "Protocollo Riservato".

8. Backup e Pulizia

8.1 Ogni utente è responsabile della corretta conservazione dei dati e dei documenti elettronici che utilizza per motivi lavorativi, di qualsiasi tipo, formato e natura essi siano. Per questo motivo la gestione dei dati sulle postazioni di lavoro (Personal computer e PC portatili) è demandata all'utente finale, che avrà l'obbligo di effettuare il salvataggio dei dati memorizzati sui computer in dotazione, con frequenza opportuna, in funzione del tipo di dati trattati, e la conservazione degli stessi in luogo idoneo. Nel caso di postazione condivisa da più utenti la corretta gestione dei salvataggi sarà cura, oltre che dei singoli utenti, anche del Dirigente Responsabile della Sezione.

8.2 Nel caso si gestiscano dati personali, per motivi di sicurezza e di privacy è sconsigliato utilizzare per il backup supporti di massa esterni (hard disk rimovibili, penne USB, DVD RW) che comunque, se utilizzati, devono essere custoditi in archivi chiusi a chiave. Sarà a cura dell'utilizzatore il rispetto del GDPR (Regolamento Europeo 2016/679) sia per quanto riguarda la gestione dei supporti rimovibili, che per la loro distruzione in caso di rottamazione.

Gli Amministratori di Sistema hanno messo a disposizione degli utenti che ne fanno richiesta, delle partizioni di disco su file server aziendali, che l'utente potrà utilizzare, in maniera esclusiva e riservata, per il salvataggio dei dati aziendali.

8.3 Le cartelle condivise sui server aziendali messe a disposizione dall'Ente vengono sottoposte a backup automatico da parte degli Amministratori di Sistema.

8.4 Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

9. Protezione antivirus

9.1 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o altro codice malware (worm, trojan, DoS, spyware, backdoor, ransomware, ecc.). E' buona norma, ad esempio, non aprire mail o relativi allegati sospetti, non navigare su siti non professionali, e così via.

La politica di sicurezza aziendale prevede l'utilizzo presso tutti i PC di un software antivirus che viene aggiornato automaticamente da internet. Non è ammesso l'utilizzo di sistemi antivirus diversi, se non espressamente autorizzati dalla Sezione "Qualità delle Prestazioni, Controllo di Gestione, Performance, Digitalizzazione e Innovazione Tecnologica".

Ogni utente è tenuto comunque a controllare la presenza e il regolare aggiornamento del software antivirus aziendale e della definizione dei virus. Nell'eventualità di PC non collegati alla rete aziendale sarà cura dell'utente provvedere al regolare aggiornamento del software.

Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito ad eliminare, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer,
- scollegare il pc dalla rete,
- segnalare l'accaduto agli Amministratori di Sistema.

9.2 Ogni dispositivo di memoria di provenienza esterna all'agenzia dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovrà essere utilizzato.

9.3 Qualora si riscontrasse da parte del dipendente il mancato rispetto di quanto sopra indicato e quindi un comportamento non corretto, ogni danno provocato dalla presenza di un malware (virus, worm, trojan horse, backdoor, spyware, dialer, ransomware, etc.) potrà essere direttamente imputabile al dipendente stesso.

10. Aggiornamento e revisione

10.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente documento tramite comunicazione alla Sezione "Qualità delle Prestazioni, Controllo di Gestione, Performance, Digitalizzazione e Innovazione Tecnologica".

10.2 Il presente documento è soggetto a revisione con frequenza annuale.