Copia

	CONSORZIO PARCO LOMBARDO DELLA VALLE DEL TICINO		
	C.d.A.	Numero 74	Data 16/11/2011
OGGETTO: APPROVAZIONE BOZZA REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI.			

VERBALE DI DELIBERAZIONE DEL CONSIGLIO DI AMMINISTRAZIONE

L'anno duemilaundici addì sedici del mese di novembre alle ore 15.00 presso la sede del Consorzio Parco Lombardo della Valle del Ticino, convocato nei modi previsti dallo statuto, si è regolarmente riunito il Consiglio di Amministrazione.
All'esame dell'argomento in oggetto, risultano presenti:

N.	COGNOME E NOME	CARICA	PRESENZE
1	BERTANI MILENA	Presidente	Presente
2	DUSE LUIGI ENZO EMILIO	Vicepresidente	Presente
3	BALESTRERI MARTA	Consigliere	Dimissionario
4	CAIELLI ROBERTO GABRIELE	Consigliere	Assente Giustificato
5	FILONI GIUSEPPE	Consigliere	Assente Giustificato
6	FRACASSI MARIO FABRIZIO	Consigliere	Presente
7	MOTTA PAOLO LUIGI	Consigliere	Presente
8	SANSON FAUSTO	Consigliere	Presente
9	TARANTINO LEONARDO	Consigliere	Dimissionario

Presiede la Sig.ra BERTANI MILENA, Presidente del Consorzio.

Assiste il segretario, Dr. Dante Miraglia

OGGETTO: APPROVAZIONE BOZZA REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI.

Deliberazione C.d.A. n. 74 del 16/11/2011

IL CONSIGLIO DI AMMINISTRAZIONE

Rilevato che in tutti gli Uffici del Consorzio Parco Lombardo della Valle del Ticino è fatto un ampio utilizzo degli strumenti informatici e telematici e che quasi tutti i dipendenti e collaboratori dell'Amministrazione dispongono di postazioni informatiche per lo svolgimento delle proprie attività professionali;

Tenuto conto che, per garantire un utilizzo corretto degli strumenti informatici e telematici, fare in modo che costituiscano efficaci strumenti di lavoro ed evitare l'insorgere di inefficienze di gestione, occorre regolamentare l'utilizzo di tali tecnologie da parte di tutti i dipendenti e collaboratori;

Ritenuto pertanto che occorre adottare un Regolamento che disciplini compiutamente l'utilizzo delle postazioni informatiche;

Richiamata la Deliberazione C.d.A. n. 25 del 01.06.2011 che ha approvato il documento programmatico sulla privacy;

Visto l'allegato "Regolamento per l'utilizzo degli strumenti informatici e telematici", che costituisce parte integrante e sostanziale del presente provvedimento;

Considerato che le disposizioni generali contenute nell'allegato Regolamento sono da attuare tramite regole tecniche che vanno emanate ed aggiornate in coerenza con il rapido evolversi delle tecnologie informatiche e telematiche;

Individuata nel Servizio Coordinamento Informatico e Servizio Statistica l'Unità organizzativa deputata ad emanare ed aggiornare tali regole tecniche e a supervisionare sulla loro corretta attuazione da parte degli Uffici;

Rilevato che l'adozione del presente Regolamento non comporta impegno di spesa o diminuzione di entrata;

Richiamati:

- l'articolo 89 del D.Lgs. 267/2000 in forza del quale ciascun Ente disciplina, con propri regolamenti, in conformità allo Statuto, l' ordinamento generale degli uffici e dei servizi, in base a criteri di autonomia, funzionalità ed economicità di gestione e secondo principi di professionalità e responsabilità;
- l'articolo 48 comma 3 del sopraccitato Decreto in virtù del quale compete all'organo direttivo l'adozione del Regolamento per l'ordinamento degli uffici e dei servizi, nel rispetto dei criteri generali stabiliti dal Consiglio;

Considerato che il vigente Statuto Consortile all'art. 10 c. 2 lett. m) attribuisce all'organo Assembleare l'adozione dei regolamenti aventi valenza esterna, mentre con l'art. 14 c. 2 lett. g) affida al Consiglio di Amministrazione l'approvazione dei regolamenti

interni, amministrativi e tecnici, necessari per il funzionamento degli uffici e dei servizi e per l'assunzione e gestione del personale;

Visti i pareri di regolarità tecnica e contabile favorevoli, allegati al presente atto ai sensi dell'art. 49, comma 1, del D.Lgs. 267/2000;

Con votazione unanime e palese;

D E L I B E R A

per le motivazioni espresse in premessa;

- di approvare il "Regolamento per l'utilizzo degli strumenti informatici e telematici", allegato alla presente deliberazione per farne parte integrante e sostanziale;

- di individuare nel Servizio Coordinamento Informatico e Servizio Statistica l'Unità organizzativa deputata ad emanare ed aggiornare le regole tecniche necessarie per l'attuazione delle disposizioni di carattere generale contenute nel Regolamento e a supervisionare sulla loro corretta attuazione da parte degli Uffici;

- di disporre che i Responsabili d'Area prestino la necessaria collaborazione affinché vengano attuate tutte le disposizioni contenute nel Regolamento citato;

- di dare atto che la presente delibera non comporta impegno di spesa o diminuzione di entrata;

Quindi,

IL CONSIGLIO DI AMMINISTRAZIONE

con successiva votazione unanime e palese

DELIBERA

di rendere il presente atto immediatamente esecutivo ai sensi e per gli effetti dell'art. 134, 4° comma del D.Lgs. 267/2000.

OGGETTO : REGOLAMENTO SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI IN DOTAZIONE AL PERSONALE DELL'ENTE.

Premessa 5
Scopo e campo di applicazione 5
Definizioni 5
Funzionamento delle risorse informatiche 6
Dati trattati attraverso le risorse informatiche concesse in dotazione 6
Utilizzo delle Postazioni di lavoro 6
Utilizzo dei supporti mobili e PC portatili 8
Utilizzo della rete LAN e delle risorse condivise 8
Utilizzo delle stampanti locali e dipartimentali 9
Acquisizione software 9
Servizi con impatto sui sistemi informatici 9
Gestione delle password e degli accessi 9
Attività di back up 10
Attività e strumenti di assistenza remota 10
Posta elettronica 11
Internet 12
Sicurezza generale e perimetrale 13
Telefonia mobile 13
Attività dell'Amministratore di Sistema 13
Osservanza delle regole sulla privacy 14
Osservanza del presente disciplinare 14
Entrata in vigore 14

F.to IL SEGRETARIO

CONSORZIO PARCO TICINO
Allegato alla deliberazione
C.D.A. n° 74 del 16.11.2021

F.to PRESIDENTE
(ENA BERTANI)

Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete tramite i personal computer, espone il Parco Ticino a rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

L'utilizzo delle risorse informatiche e telematiche dell'Ente deve sempre ispirarsi al principio di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro.

Il personal computer, i relativi programmi e/o applicazioni e/o dati ed archivi affidati in uso ai dipendenti sono strumenti di lavoro di proprietà dell'Ente. Tutto quanto messo a disposizione, ricevuto, rilasciato e comunque memorizzato sul posto di lavoro e sui mezzi di comunicazione è e rimane di proprietà dell'Ente.

Il Garante della Privacy è intervenuto sul tema dell'utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet con il provvedimento n. 13 del 1° marzo 2007, indicando ai datori di lavoro le linee guida da adottare a garanzia degli interessi del personale dipendente, garantendo l'adozione delle misure di sicurezza idonee ad assicurare la disponibilità e l'integrità dei sistemi informativi e dei dati.

Inoltre lo Statuto dei Lavoratori (L.300/70) all'art. 4 prevede che

> *"Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna."*

Scopo e campo di applicazione

Alla luce di quanto premesso, il Parco Ticino adotta il presente disciplinare interno al fine di

- evitare comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati
- informare il personale dipendente di quali sono le misure di tipo organizzativo e tecnologico adottate dall'Ente per la sicurezza dei dati
- informare il personale dipendente su come vengono trattati i dati relativi all'uso dei mezzi informatici per la tutela dei lavoratori.

Questo documento non si riferisce solamente all'utilizzo di internet o della rete locale, ma si riferisce a tutto l'insieme delle risorse informatiche, di calcolo, di comunicazione, elettroniche, audiovisive e a qualsiasi altra tipologia di risorsa presente nell'Ente.

Tutti i contratti che verranno conclusi tra l'Ente e terzi soggetti a cui viene permesso l'accesso ai dati, ai programmi informatici o ad altri mezzi dell'Ente, dovranno riportare una clausola che impegni le parti a rispettare il presente documento; ciò indipendentemente dalla nomina a incaricato o a responsabile del trattamento dati ai sensi del D. Lgs. 196/2003.

Nel caso di soggetto esterno nominato responsabile del trattamento, questi deve impegnarsi a far rispettare il presente documento a tutti i propri dipendenti e ad eventuali altri soggetti.

Definizioni

TITOLARE DEL TRATTAMENTO DEI DATI: è la figura individuata dall'art. 28 del Decreto Legislativo 30 giugno 2003, n. 196. Vigila sulla puntuale osservanza di tutte le disposizioni in materia di trattamento dei dati. Designa tutte le altre figure coinvolte nel trattamento informatico dei dati.

RESPONSABILE DEL TRATTAMENTO: è la figura prevista dall'art. 29 del Decreto Legislativo 30 giugno 2003, n. 196 ed è nominata dal Titolare. Garantisce il pieno rispetto delle vigenti disposizioni in materia di trattamento (anche informatico) dei dati; i compiti affidati al responsabile sono analiticamente specificati per iscritto dal Titolare al momento della nomina.

RESPONSABILE DEI SERVIZI INFORMATICI: è la figura, designata dal Titolare, che gestisce e coordina le attività di configurazione/aggiornamento dei sistemi e degli archivi informatici. Il ruolo del Responsabile è quello di coordinatore dell'applicazione della normativa sulla sicurezza dei dati dal punto di vista informatico. La figura di Responsabile dei servizi informatici è ricoperta dal Responsabile di Area che gestisce la promozione e gestione dei sistemi informatici e telematici.

AMMINISTRATORI DI SISTEMA: sono le figure, designate dal Titolare, che provvedono operativamente alla gestione e manutenzione del sistema informatico dell'Ente sulla base delle misure organizzative fissate dal responsabile dei servizi informatici.

INCARICATI DEL TRATTAMENTO: è la figura prevista dall'art. 30 del Decreto Legislativo 30 giugno 2003, n. 196 ed è nominata dal Titolare o dal Responsabile del trattamento; tratta i dati sia in forma cartacea sia attraverso strumenti informatici; opera sotto la diretta autorità del Responsabile del trattamento, attenendosi alle istruzioni impartite.

INCARICATO BACKUP: è individuato dal Responsabile di Area/Servizio e si occupa delle operazioni di backup dei dati sulla base delle istruzioni impartite dall'Amministratore di Sistema; per questa particolare mansione risponde direttamente all'Amministratore di Sistema; la sua designazione è effettuata per iscritto.

CUSTODE DELLE PASSWORD: ove i sistemi informatici o le banche dati, non consentano una gestione automatizzata delle password (come avviene nell'Active Directory di Windows) e sia necessario tenere traccia delle password per iscritto, viene nominato uno i più custodi delle password che provvedono a conservare le password che vengono consegnate dagli utenti in busta chiusa.

TRACCIAMENTO: memorizzazione di eventi e operazioni effettuata automaticamente da un qualsivoglia dispositivo informatico, per finalità manutentive e di funzionamento dello stesso.

RILEVAZIONE: complesso di operazioni di analisi e verifica dei tracciamenti effettuati dai dispositivi svolte da Amministratori di Sistema a fronte di comprovate necessità definite nei capitoli seguenti del presente disciplinare.

Funzionamento delle risorse informatiche

Le risorse informatiche tracciano una serie di eventi di sistema per attività amministrative, manutentive e/o di sicurezza, che variano a seconda della tipologia delle risorse stesse.
Il tracciamento di tali eventi non è generalmente oggetto di rilevazione da parte del servizio informatico. Qualora, per necessità manutentive o di gestione della sicurezza si renda necessario rilevare e/o registrare gli eventi tracciati di una risorsa specifica, tali trattamenti verranno preventivamente segnalati al personale aziendale nelle modalità indicate nei successivi paragrafi.

Dati trattati attraverso le risorse informatiche concesse in dotazione

Gli unici dati che potranno essere trattati dagli utenti tramite le risorse informatiche messe a disposizione dell'azienda sono di carattere professionale.
E' vietato qualsiasi utilizzo personale delle attrezzature concesse in dotazione.
Pertanto, qualsiasi dato e informazione gestiti tramite le risorse oggetto del presente disciplinare sono da considerarsi di proprietà dell'Ente.
Alla riconsegna delle attrezzature da parte degli utenti all'Ente, questo potrà liberamente disporre di eventuali informazioni ivi presenti.

Utilizzo delle Postazioni di lavoro

La postazione di lavoro affidata al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente l'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza per cui va assolutamente evitato l'utilizzo personale dello stesso.
Non è consentito installare programmi provenienti dall'esterno salvo preventiva autorizzazione da parte di un Amministratore di Sistema, onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli messi a disposizione dall'Ente stesso, in quanto l'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili e penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (Legge 633 del 22 aprile 1941 sulla tutela della proprietà intellettuale, D.Lgs. 29 dicembre 1992 n. 518, sulla tutela giuridica del software e aggiornamenti successivi) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Il personal computer (di seguito denominato PC) viene consegnato all'utente con una configurazione coerente con le misure organizzative e di sicurezza impostate dall'Ente stesso: non è consentito all'utente di modificare le caratteristiche impostate sul PC, salvo preventiva autorizzazione da parte di un Amministratore di Sistema.

Il PC deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio, salvo specifica disposizione dell'Amministratore di Sistema e/o a seguito di pianificazione dello spegnimento automatico. In ogni caso, poiché 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'uso indebito, l'utente che si allontana dalla postazione deve bloccarne l'uso tramite la combinazione dei tasti CTRL + ALT + CANC e successivo INVIO. Si consiglia di attivare lo screen saver con la richiesta di password per lo sblocco con avvio automatico dopo 15 minuti di non utilizzo della postazione.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna. Prima dell'apertura del supporto deve provvedere alla sua scansione tramite il software antivirus. L'utente deve avvertire immediatamente un Amministratore di Sistema nel caso in cui vengano rilevati virus.

Non è consentito l'utilizzo di giochi o altre applicazioni di tipo ludico anche se comprese nel sistema operativo installato.

Non sono permesse, a meno di specifiche e documentate autorizzazioni le seguenti attività:

- caricare, memorizzare, pubblicare, diffondere, distribuire, tramite risorse dell'Ente documenti, informazioni, immagini, filmati ecc. in generale, ed in particolare:
    - a carattere violento, pornografico o contrario alla pubblica decenza, o suscettibile di mancare di rispetto agli esseri umani o alla loro dignità, con contenuto discriminatorio razziale ed etnico, contrario al buon costume, oltraggioso nei confronti dei minori, contrario all'ordine pubblico, diffamatorio o che contenga contenuti illeciti penalmente o civilmente riconducibili a categorie qui non espressamente indicate;
    - pregiudizievoli per le risorse dell'Ente e per l'integrità e la conservazione dei dati dell'Ente stesso;
    - pregiudizievoli per l'immagine e il buon nome dell'Ente all'esterno dell'Ente;
- accedere a server web trattanti materie o soggetti ricadenti nelle categorie sopra elencate;
- tenere comportamenti che possano indurre taluno ad effettuare invii di materiale rientrante nelle tipologie sopra elencate; laddove l'utente si trovi a ricevere anche contro il suo volere tali materiali, è tenuto a informare il Responsabile del Sistema Informativo e attenersi alle sue istruzioni circa il trattamento di tali materiali;
- utilizzare le risorse dell'Ente con fini di molestia, minaccia o comunque violando le norme di legge in vigore;
- caricare, memorizzare, trasmettere o utilizzare programmi, software, procedure od altra utilità che siano protetti dalle leggi sulla proprietà intellettuale, salvo che il Parco Ticino ne detenga regolare licenza e/o autorizzazione del produttore;
- utilizzare strumentazioni, programmi, software, procedure, ecc. messi a disposizione dall'Ente in violazione delle Leggi sulla proprietà intellettuale, delle regole di buona tecnica applicabili e delle prescrizioni emanate dall'Ente;
- caricare o trasmettere, con volontà, archivi o programmi contenenti virus o dati alterati;
- manomettere sistemi o archivi in maniera tale da inficiare la riservatezza, la disponibilità e/o l'integrità dei dati;
- inviare messaggi in massa ("spam") o favorire il propagarsi di notizie riconducibili a ciò che abitualmente viene definito "catena di S. Antonio";
- utilizzare le risorse dell'Ente in modo da consentire a soggetti non abilitati l'accesso ai dati e ad alle informazioni riservate, se non nei casi espressamente previsti dalla Legge e dai Regolamenti.

Poiché alcune attività sopra elencate possono avere conseguenze di natura penale, esse originano in capo al trasgressore tutte le responsabilità previste dalla Legge.

Nonostante la presenza di programmi antivirus, è ritenuto statisticamente probabile che l'utilizzo di applicazioni di comunicazione (internet, posta elettronica, ecc.) e di supporti magnetici rimovibili (floppy, CD, ecc.) comporti la trasmissione di virus informatici o di programmi e archivi in grado di alterare, distruggere o monitorare l'attività e i contenuti dei personal computer.

In caso di anomalie dell'hardware e del software affidatogli, l'utente deve immediatamente bloccarne l'operatività, fermare le eventuali elaborazioni in corso ed informare immediatamente il Servizio Informatico per le incombenze di competenza.

Utilizzo dei supporti mobili e PC portatili

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, secure drive, cd, dvd, chiavi e dischi esterni USB, ecc...) contenenti dati personali devono essere utilizzati con particolare cautela onde evitare che il loro contenuto possa essere trattato da soggetti non incaricati.

Ogni dipendente sarà ritenuto direttamente responsabile di qualsiasi trattamento inadeguato di dati derivante da un suo improprio utilizzo dei supporti.

L'utente è responsabile delle attrezzature informatiche portatili assegnategli dal servizio informatico e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai portatili si applicano le regole di utilizzo previste per i PC connessi alla rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

Gli utenti di PC portatili si impegnano, dovunque dovessero trovarsi, a mettere in sicurezza la strumentazione di cui hanno l'uso e i dati nella stessa contenuta.

Danni arrecati alle attrezzature ed ai PC o la loro perdita dovuta ad incauta custodia saranno a carico dell'utente utilizzatore.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna. Prima dell'apertura del supporto deve provvedere alla sua scansione tramite il software antivirus. L'utente deve avvertire immediatamente un Amministratore di Sistema nel caso in cui vengano rilevati virus.

Utilizzo della rete LAN e delle risorse condivise

Al fine di garantire la disponibilità dei dati e un'efficace politica di backup, gli utenti devono salvare su cartelle di rete tutti i file di lavoro ed astenersi dal salvarli sul disco locale della postazione di lavoro (si specifica che la cartella "desktop" si trova sulla postazione in locale, pertanto è inadatta al salvataggio dei file perché non sottoposta a procedure di backup).

Le cartelle/unità di rete 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.

Sulle cartelle/unità di rete vengono svolte regolari attività di amministrazione e backup.
Le password di ingresso alla rete ed ai programmi sono personali: è assolutamente vietato entrare nella rete e nei programmi con profili assegnati ad altri utenti.

L'Amministratore di Sistema, nell'espletamento delle mansioni attribuitegli dal Responsabile dei servizi informatici, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza, sia sui PC degli incaricati sia sui server.
Per la trasmissione di file all'interno dell'Ente è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, oppure è possibile utilizzare le cartelle di scambio create a tale scopo. Le cartelle di scambio devono essere tenute in ordine, eliminando i file non più necessari anche al fine di non consentire il trattamento dei dati a persone non espressamente incaricate.

Il File System a disposizione degli utenti è così composto:

- Disco H: (Home) – directory di lavoro personale
- Disco K: directory di lavoro della propria area/settore
- Disco I (Intranet) – directory di scambio dei dati con altri uffici
- Disco S (Siscom, opzionale) – applicativi delibere e determinazioni

Gli utenti dovranno effettuare la stampa dei dati solo se strettamente necessaria e dovranno ritirarla prontamente dai vassoi delle stampanti comuni.

Il collegamento alla rete comunale di personal computer portatili o di attrezzature informatiche non di proprietà del Parco Ticino è vietato.

Il Servizio Informatico potrà consentire deroghe a quanto previsto dal precedente paragrafo solo dopo attenta valutazione da parte del personale tecnico informatico.

Utilizzo delle stampanti locali e dipartimentali

Il sistema informatico dell'Ente è composto anche da strumentazioni di stampa per lo più dipartimentali. L'utilizzo di queste risorse è esclusivamente lavorativo, ne è fatto divieto l'utilizzo per la riproduzione di proprio materiale nonché per la stampa di materiale non prettamente inerente l'ambiente lavorativo.

Ogni dipendente del consorzio viene dotato di un codice di stampa al quale è stato assegnato una soglia di stampe/riproduzioni da poter effettuare. L'aumento della soglia deve essere richiesto all'ufficio Sistemi Informatici che provvederà, previa autorizzazione dal responsabile, all'aumento della stessa.

Acquisizione software

Sulle postazioni è consentita l'installazione esclusiva delle seguenti categorie di software:

- software commerciale dotato di licenza d'uso (es. pacchetti di Office Automation)
- software gestionale utilizzato specificatamente all'interno del Parco Ticino fornito dalle ditte specializzate nel settore della P.A. (es. applicativi in uso ai vari servizi)
- software realizzato specificatamente dagli organi centrali della Pubblica Amministrazione o Enti nazionali (es. INPS, Ministeri...)
- software gratuito (freeware) e shareware prelevato dai siti internet, solo se espressamente autorizzato da un Amministratore di Sistema
- qualsiasi altro software si renda necessario per l'esercizio delle attività lavorative e istituzionali.

L'acquisto e la conseguente installazione di software devono essere sempre preventivamente valutati, autorizzati ed effettuati in collaborazione col Servizio Informatico, al fine di garantire la stabilità dei sistemi e la compatibilità del software con gli stessi.

Servizi con impatto sui sistemi informatici

L'acquisizione di materiale hardware o di qualsiasi dispositivo che interagisca con la rete e/o la strumentazione informatica dell'ente può avere un impatto con essi, qualora non venga eseguita direttamente dal servizio informatico, deve essere concordata preventivamente con questo, onde evitare disfunzionamenti, cadute prestazionali o altri problemi alla sicurezza e all'immagine dell'Ente stesso.

Qualora nell'esercizio di una funzione amministrativa sia prevista la fornitura di software accessorio alla gestione/erogazione di un servizio, l'ufficio competente deve consultare il Servizio Informatico nelle fasi preliminari del processo di acquisizione per la corretta definizione delle caratteristiche del software, affinché lo stesso risulti:

- compatibile con il sistema informatico del Parco,
- conforme alle misure di sicurezza adottate dall'Ente con particolare riguardo alla sicurezza degli accessi,
- certificato per l'installazione sulle macchine in dotazione all'Ente (server e pc),
- installato correttamente.

In caso di mancata consultazione preventiva del servizio informatico non verrà effettuata alcuna installazione.

Qualora venga affidata all'esterno la gestione di dati dell'Ente per l'erogazione di servizi, l'ufficio competente deve concordare preventivamente con il Servizio Informatico le modalità e i formati con cui questi dati devono essere scambiati sia in ingresso che in uscita e le condizioni di consegna dei dati al termine del rapporto di collaborazione.

Gestione delle password e degli accessi

L'utente deve utilizzare sempre una password quando viene richiesto dalle procedure in uso, avendo cura che nessuno ne venga a conoscenza.

La password di ingresso al dominio (ed eventualmente dello screensaver) sono previste e vengono attribuite da un Amministratore di Sistema all'utente per il primo accesso. Dopo il primo accesso il sistema chiederà all'utente di modificare la password, la quale sarà conosciuta solo dall'utente stesso. Qualora si renda necessario (per manutenzione, aggiornamenti, assenza prolungata imprevista che renda indisponibili risorse gestite dall'utente) che un Amministratore debba entrare nel sistema con il profilo dell'utente, verrà modificata la password di accesso dell'utente stesso. Al successivo accesso da parte dell'utente l'Amministratore rilascerà una password di cortesia che verrà immediatamente modificata dall'utente stesso.

L'accesso agli applicativi può a sua volta essere regolato da un'ulteriore password: le modalità di gestione e di scadenza della password sono specifiche per ogni programma. All'utente sarà fornito un profilo personale e verranno attivate procedure per garantire all'utente stesso la conoscenza esclusiva della propria password. Nel caso il sistema non lo consenta o sia necessario l'intervento di un Amministratore di Sistema per garantire la disponibilità dei dati, verranno concordate procedure specifiche per la gestione degli accessi fra il Responsabile del Sistema Informatico e il Responsabile del Trattamento.

La combinazione dell'accesso al dominio e agli applicativi garantirà il rispetto delle regole minime di sicurezza indicate nel Codice della Privacy.

Le password del dominio e degli applicativi, salvo impossibilità dovute all'obsolescenza del software, devono essere modificate ogni 3 mesi, devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato.
Nel caso in cui si sospetti che una password abbia perso la segretezza, l'utente provvederà ove possibile a modificarla personalmente, altrimenti provvederà a modificarla con il supporto dell'Amministratore di Sistema.

Non è consentito utilizzare il profilo personale di altri soggetti per connettersi al dominio o agli applicativi. Qualora l'utente venisse a conoscenza delle password di un altro utente, è tenuto a darne immediata notizia ad un Amministratore di sistema.

Come indicato al punto 7 dell'Allegato B del Codice della Privacy "Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica".

Attività di back up

Sono oggetto di attività di salvataggio centralizzato su supporti magnetici o ottici:

- i file salvati sulle cartelle/unità di rete messe a disposizione dal Servizio Informatico;
- le banche dati di applicativi ed i relativi file di sistema;
- le caselle di posta elettronica.

Gli elementi sopra indicati vengono salvati sistematicamente ogni notte (5 volte la settimana).

I dati che risiedono sulle postazioni PC non sono soggetti a operazioni di backup centralizzato.

Le modalità di salvataggio dei dati comportano la registrazione dei dati su supporti ottici o magnetici per un massimo di 6 mesi.

Attività e strumenti di assistenza remota

Per finalità di carattere manutentivo sono attivi presso l'Ente strumenti di assistenza remota che consentono agli Amministratori di Sistema di connettersi alle postazioni degli utenti per fornire supporto in tempo reale a assistere gli utenti nella risoluzione di problematiche di carattere informatico.
Gli strumenti utilizzati manifestano esplicitamente la connessione alla postazione da parte dell'Amministratore: l'utente dovrà consentire tramite autorizzazione verbale o informatica l'intervento remoto.
Per quanto riguarda gli interventi di assistenza remota sulle postazioni da parte di Amministratori esterni, detti interventi dovranno comunque essere preventivamente concordati con il Servizio Informatico e comunque comunicati al servizio stesso.

Posta elettronica

La casella di posta elettronica, assegnata dall'Ente all'utente, è uno strumento di lavoro.
Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Qualsiasi attività istituzionale realizzata tramite utilizzo di posta elettronica deve essere svolta con l'esclusivo utilizzo di caselle registrate sotto il dominio di posta istituzionale dell'Ente o tramite caselle di posta elettronica certificata registrate dall'Ente stesso.

E' fatto divieto di utilizzare le caselle di posta elettronica istituzionali per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione da parte del Responsabile dei Servizi Informatici per esigenze di lavoro.
E' inoltre da evitare ove possibile l'invio di messaggi con allegati di grandi dimensioni al fine di evitare eventuali sovraccarichi al sistema informativo e nuocere all'efficacia della comunicazione.

La casella di posta deve essere tenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Per la trasmissione di file all'interno dell'Ente è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, oppure è possibile utilizzare le cartelle di scambio create a tale scopo.

E' vietato inviare mail con allegati contenenti file eseguibili (estensione .exe, .bat, ecc.).

E' vietato inviare catene telematiche (o di S. Antonio). Se si dovessero ricevere messaggi di tale tipo, si dovrà cancellare il messaggio ricevuto senza divulgarlo in alcun modo. Non si dovranno in alcun caso attivare gli allegati di tali messaggi.

Qualora si ricevessero messaggi sospetti di richiesta di password o altre informazioni oppure di invito a svolgere operazioni sulla propria postazione di lavoro (es. apertura o cancellazione di file, installazione aggiornamenti, ecc) di cui non è certa la provenienza, l'utente è tenuto a segnalarli immediatamente all'Amministratore di Sistema prima di effettuare qualsiasi azione.

Al fine di garantire la continuità di servizio, sono previste 2 differenti modalità per la gestione delle assenze, programmate o non, degli operatori preposti alla lettura dei messaggi di una specifica casella di posta:

1) ASSENZA PROGRAMMATA: attivazione di un risponditore automatico che segnali la temporanea indisponibilità all'accesso alla casella di posta, indicando eventualmente una casella di posta alternativa a cui inviare il messaggio. Tale attivazione può essere svolta dall'utente stesso o da un Amministratore di Sistema appositamente incaricato;
2) ASSENZA NON PROGRAMMATA: l'utente è comunque obbligato, anche in caso di assenza non programmata, a collegarsi al sistema di posta elettronica e ad attivare il risponditore automatico come indicato al punto precedente. In caso di necessità, su specifica richiesta al Responsabile dei Servizi Informativi da parte del responsabile dell'utente assente, quest'ultimo verrà contattato da un Amministratore di Sistema il quale gli chiederà l'esplicito permesso verbale di accesso alla casella di posta elettronica. A seguito di tale assenso, l'Amministratore di Sistema provvederà ad inoltrare al responsabile o ad un suo incaricato i messaggi di posta ritenuti necessari. In caso di impossibilità di raggiungere l'utente assente, il suo responsabile potrà richiedere all'Amministratore di Sistema di accedere alla casella di posta dell'utente assente, richiedendo l'inoltro dei messaggi ritenuti necessari per lo svolgimento delle attività lavorative; tale richiesta dovrà essere preventivamente autorizzata dal Responsabile dei Sistemi Informativi o, in caso di sua assenza, da chi ne fa le veci. Al termine dell'operazione, l'Amministratore di Sistema redigerà un rapporto dell'intervento effettuato in cui saranno riportati gli estremi dell'autorizzazione ad intervenire. Tale rapporto di intervento verrà inviato all'utente assente, al suo responsabile e al Responsabile dei Servizi Informativi.

E' vietato utilizzare client di posta elettronica differenti da quelli installati e configurati dagli Amministratori di Sistema.

Le caselle di posta elettronica in uso presso l'Ente sono di 2 tipologie:

1) caselle nominative, assegnate con la convenzione *<nome.cognome>*@parcoticino.it Tali caselle sono intestate personalmente agli utenti: è importante sottolineare che, nonostante le caselle siano intestate ad un individuo, sono da considerarsi uno strumento aziendale e non corrispondenza privata; pertanto, l'utilizzo verso destinatari esterni dovrà essere consono con le funzioni istituzionali svolte dall'Ente. La divulgazione dell'indirizzo di posta nominativo deve essere limitata ai soli casi in cui non possa essere divulgato l'indirizzo di posta relativo all'ufficio o alla funzione di appartenenza. In caso di attività di servizio nella corrispondenza interna fra uffici dell'Ente, il mittente potrà inviare la mail utilizzando la richiesta di conferma di ricezione da parte dei destinatari, i quali dovranno confermare l'avvenuta ricezione del messaggio.

2) Caselle di posta assegnate ad un ufficio o ad una funzione sul dominio @parcoticino.it . Tali caselle sono configurate per lo scambio di posta verso l'esterno e possono essere assegnate ad una o più persone. In caso siano assegnate ad una sola persona, questa ha la responsabilità di garantire la continuità nella gestione della corrispondenza; in caso di sua indisponibilità, programmata o non, verrà attivata una delle 2 differenti modalità per la gestione delle assenze indicate precedentemente. In caso di caselle di posta assegnate a più persone, la continuità nella gestione della corrispondenza e delle attività ad essa correlate dovrà essere assicurata dal Responsabile del Trattamento dei dati attraverso opportune scelte organizzative.

L'Amministratore di Sistema, nell'espletamento delle sue funzioni, potrà accedere alle caselle di posta assegnate per finalità manutentive solo in presenza dell'assegnatario (o su sua esplicita autorizzazione) della casella o su richiesta del diretto superiore in caso di indisponibilità dell'assegnatario.

L'Ente si impegna in ogni caso a rispettare la confidenzialità dei messaggi elettronici di provenienza o a destinazione di recapiti sindacali (contenuto, autori e destinatari), delle mailing list elaborate e scambiate in rete da organismi sindacali, ecc.

Internet

Il collegamento ad Internet è uno strumento messo a disposizione per i soli scopi di lavoro: è proibita la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza per cui va assolutamente evitato l'utilizzo personale dello stesso.

Pertanto, per garantire quanto previsto dalla Legge e secondo le direttive emanate dal Garante per la tutela e protezione dei dati, al fine di evitare abusi e evitare il monitoraggio del traffico telematico, è attivato un filtro che blocca l'accesso ai siti ritenuti palesemente non pertinenti con le attività istituzionali. Qualora, per lo svolgimento della attività istituzionali, un utente necessitasse di accedere a un sito scartato dai sistemi di filtraggio, potrà richiedere per tramite del Responsabile del Trattamento (che ne assume la responsabilità) al Responsabile del Sistema Informatico l'accesso a tale sito.

E' fatto assoluto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato dai siti internet, se non espressamente autorizzato da un Amministratore di Sistema.

E' tassativamente vietato qualsiasi genere di transazione privata in campo finanziario ivi comprese le operazioni di remote banking, acquisti online e simili.

E' tassativamente vietata ogni forma di registrazione e connessione a siti i cui contenuti non siano legati all'attività lavorativa.

E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line, di blog, di bacheche elettroniche e in generale di strumenti di social network anche utilizzando pseudonimi (o nicknames), esclusi gli strumenti autorizzati per esigenze di lavoro.
A fini statistici, di qualità del servizio e di sicurezza, l'occupazione di banda generata dal traffico internet e dallo scambio di posta elettronica è soggetta a periodiche verifiche e controllo da parte dell'Ente sotto forma di dati aggregati ed anonimi, in osservanza dei limiti posti dalla legge in materia di riservatezza.

Qualora i sistemi di sicurezza segnalino delle potenziali criticità che possano minare l'integrità dei dati e la stabilità del sistema stesso, potrebbero essere effettuati dei controlli sulla navigazione internet. Tali controlli saranno preventivamente segnalati al personale e si opereranno secondo stadi successivi:

1) controlli generici sulle pagine visitate, senza che vengano tracciati gli utenti che le visitano;
2) controlli aggregati sulle pagine visitate con suddivisione del traffico effettuato per aree;
3) controlli specifici sulle pagine visitate, con tracciamento dell'indirizzo IP da cui si effettua la visita o dell'utente che la effettua.

Il tracciamento specifico verrà effettuato solo qualora il trattamento generico e quello aggregato non abbiano consentito di risolvere le criticità riscontrate e verrà comunque nuovamente segnalato in forma preventiva agli utenti.

Per quanto riguarda l'utilizzo di chiavi USB per la navigazione internet, l'Ente non attuerà alcuna rilevazione delle pagine visitate e si limiterà, in caso di necessità, al controllo dei costi di traffico. Gli utenti che verranno dotati di tali strumenti dovranno attenersi comunque a norme di comportamento adeguate ai principi su cui si basa il presente disciplinare e saranno comunque responsabili di qualsiasi azione svolta tramite l'utilizzo di tali strumenti. L'Ente, in caso di necessità, renderà disponibile la documentazione amministrativa attestante il rilascio e il ritiro di tali risorse agli utenti.

Sicurezza generale e perimetrale

Presso l'Ente è attivato un sistema di sicurezza perimetrale a difesa dei sistemi e dei dati, che traccia eventi che possono essere indizio di minacce informatiche. Il sistema è soggetto a procedure di aggiornamento automatico per quanto riguarda la lista e le caratteristiche delle minacce.

E' gestito dal Servizio Informatico, il quale effettua attività di verifica delle segnalazioni attivate dal sistema stesso, con lo scopo di comprendere e prevenire eventuali minacce esterne.

Qualora il sistema attivato rilevi delle minacce a specifici indirizzi IP interni delle postazioni di lavoro, il Servizio Informatico ne verificherà la natura insieme all'utente/utenti che abitualmente utilizza/utilizzano la postazione, con l'obiettivo di comprendere la natura della minaccia e prevenire eventuali danni.

Una volta individuate le cause dell'evento rilevato verranno adottati provvedimenti correttivi, con segnalazione al Titolare dei Trattamenti di eventuali violazioni alle regole indicate nel presente disciplinare.

Telefonia mobile

I dispositivi di telefonia mobile eventualmente forniti dall'Ente a dipendenti costituiscono uno strumento di lavoro e/o attività istituzionale. L'Ente potrà richiedere il rimborso delle spese imputabili ad utilizzi personali dello strumento.

I consumi telefonici di ogni dispositivo potranno essere analizzati dall'Ente in forma aggregata ai fini di controllo e contenimento dei costi di esercizio: qualora i consumi si dovessero rivelare non conformi rispetto a quanto atteso per l'attività svolta, l'Ente potrà richiedere all'utente a cui è stato affidato il dispositivo di evidenziare le voci di spesa personali, al fine di imputargli tali spese. I numeri presenti nei dati di traffico saranno oscurati nelle ultime tre cifre, per cui non sarà possibile risalire ai numeri contattati.

Per gli altri aspetti concernenti i consumi telefonici e il traffico internet generati sui dispositivi si rimanda alle norme comunicate in fase di assegnazione del bene o in fasi successive al variare delle condizioni di assegnazione.

A causa delle sempre maggiore interazione tra i dispositivi telefonici e informatici, l'abuso di tali strumenti può costituire una potenziale fonte di minaccia ai sistemi dell'Ente. Pertanto è vietato:

- utilizzare i dispositivi per navigare in Internet presso siti che esulino dalle attività istituzionali;

- installare applicazioni sui dispositivi cellulari senza prima aver concordato la cosa con il Servizio Informatico;

- installare sulle postazioni di lavoro in ufficio programmi di sincronizzazione/backup dei dati contenuti sui dispositivi cellulari senza la preventiva autorizzazione del Servizio Informatico.

Al momento della restituzione dei dispositivi, il personale assegnatario dovrà cancellare i dati contenuti sul cellulare (es. Rubrica telefonica, SMS, contenuti multimediali, ecc). Qualora il dispositivo restituito contenga dati personali, questi verranno cancellati indiscriminatamente dal Servizio Informatico prima di un'eventuale assegnazione successiva.

Attività dell'Amministratore di Sistema

S'intende per Amministratore di Sistema qualsiasi soggetto le cui funzioni di gestione ed amministrazione di sistemi informatizzati rendano ad esso tecnicamente possibile l'accesso, anche fortuito, a dati personali. In questa definizione rientrano pertanto le funzioni tecnicamente definite di amministratore di sistema (*system administrator*), amministratore di base di dati (*database administrator*) o amministratore di rete (*network administrator*).

L'Amministratore di Sistema è designato dal Titolare in forma scritta. La designazione quale Amministratore di sistema deve essere conforme alle normative sulla protezione dei dati personali e ai provvedimenti relativi emanati dal Garante della Privacy sull'argomento.

Deve inoltre recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Fra le funzioni dell'Amministratore di sistema, sia esso interno all'Ente che esterno, vi possono essere:

- sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- effettuare e/o coordinare interventi di manutenzione hardware per i dispositivi di competenza;

- effettuare interventi di manutenzione software su sistemi operativi e applicativi di competenza;
- coordinare e sovrintendere l'operato di eventuali tecnici esterni all'Amministrazione (nel caso di Amministratore interno);
- coordinare a livello operativo la gestione e la distribuzione dei profili di accesso e delle password degli utenti del sistema e/o dei sottosistemi di competenza nel rispetto delle normative relative alla protezione dei dati personali;
- gestire le password di amministrazione di sistema o dei sottosistemi di competenza;
- collaborare con i responsabili del trattamento dei dati personali per l'organizzazione delle politiche di sicurezza;
- informare il responsabile dei sistemi informatici e/o il titolare sulle non corrispondenze con le norme di sicurezza e su eventi di sicurezza rilevanti.

Osservanza delle regole sulla privacy

Oltre a quanto indicato nel presente documento, è obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza ai sensi dell'allegato tecnico B al Decreto Legislativo 196/2003 e normative successive.

Osservanza del presente disciplinare

La finalità del presente documento è quella di regolamentare l'utilizzo delle risorse informatiche aziendali, al fine di garantire l'adeguata riservatezza, integrità e disponibilità dei dati gestiti dall'azienda.

A tali scopi, in caso si riscontrino delle criticità che possano ledere la sicurezza del sistema informativo, l'Ente potrà verificare che l'utilizzo delle risorse informatiche concesse in dotazione agli utenti sia conforme alle indicazioni riportate nel presente disciplinare. Qualora l'utilizzo delle risorse informatiche possa in qualche maniera rivelare dati personali relativi agli utilizzatori, la rilevazione verrà effettuata secondo i principi di pertinenza e non eccedenza del trattamento dei dati rispetto alle finalità di sicurezza per cui tali dati sono trattati.

Il mancato rispetto delle regole e delle misure di sicurezza elencate nel presente documento implica la responsabilità personale dell'utente.

I fatti negativi e/o pregiudizievoli espongono il trasgressore oltre che all'apertura di specifico procedimento disciplinare, alle sanzioni previste dalla legge.

Entrata in vigore

Il presente documento è in vigore a partire dal 16/11/2011.

Gli uffici competenti provvederanno a consegnare al momento dell'assunzione ad ogni utente copia del presente disciplinare.

CONSORZIO PARCO LOMBARDO DELLA VALLE DEL TICINO

Sviluppo sostenibile

Tutela della biodiversità e dell'ambiente, qualità della vita

Proposta Consiglio d'Amministrazione N.425 del 27/10/2011

Deliberazione C.D.A N° 74 del 16/11/2011

Oggetto:
APPROVAZIONE BOZZA REGOLAMENTO PER L L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI

Sulla proposta di deliberazione i sottoscritti esprimono ai sensi dell'art.49, 1° comma del D.Lgs. 18 agosto 2000, n. 267, i pareri di cui al seguente prospetto:

Visto del responsabile del procedimento Tiziana Vecchio

Parere	Testo	Esito	Data	Responsabile	Firma
TECNICO	PARERE IN ORDINE ALLA REGOLARITA' TECNICA	Favorevole	04/11/2011	TIZIANA VECCHIO	
CONTABILE	PARERE IN ORDINE ALLA REGOLARITA' CONTABILE	Favorevole	04/11/2011	TIZIANA VECCHIO	

Note:

Il presente verbale di deliberazione viene letto, approvato e sottoscritto come segue:

IL PRESIDENTE
F.to: Milena Bertani

IL SEGRETARIO
F.to: Dr. Dante Miraglia

Copia conforme all'originale, per uso amministrativo.
Magenta , lì 23 NOV 2011
23 NOV 2011

CONSORZIO PARCO LOMBARDO VALLE TICINO - MAGENTA -

IL RESPONSABILE DELL'AREA AMMINISTRATIVA, FINANZIARIA E LEGALE

RELAZIONE DI PUBBLICAZIONE

Su conforme certificazione dell'Ufficio Messi del Comune di Magenta si attesta che il presente atto è stato pubblicato all'Albo Pretorio online del Comune stesso, ai sensi dell'art. 32 della legge 29/2009.

dal 24 NOV 2011 al 09 DIC 2011

Magenta, _____

IL SEGRETARIO

ATTESTAZIONE DI ESECUTIVITA'

Pubblicata all'Albo Pretorio del Comune di Magenta il _____ la presente deliberazione è divenuta esecutiva ai sensi delle vigenti disposizioni di legge essendo decorsi 10 giorni dalla data di inizio della pubblicazione.

Magenta, _____

IL SEGRETARIO