

**DISCIPLINARE PER IL CORRETTO USO  
DELLE RISORSE INFORMATICHE E  
TELEMATICHE CONSORTILI**

**Approvato con decreto del Commissario Straordinario  
n. 55 del 26/04/2012**

## **PREMESSA**

Il Consorzio di Bonifica del Padule di Fucecchio promuove l'uso delle risorse informatiche e telematiche, quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in un'ottica di semplificazione dell'attività amministrativa, secondo quanto previsto dal Codice dell'Amministrazione digitale.

In un contesto di esponenziale crescita dei dati trattati e dei rischi connessi, è fondamentale disporre di un adeguato sistema di protezione del patrimonio informativo del Consorzio che ne tuteli la riservatezza e la sicurezza.

“La sicurezza non è contraddittoria alla privacy ma è invece l'unica minima garanzia e speranza che io possa avere che siano tutelati i dati dei cittadini nel contesto di così crescente bulimia e richiesta di dati.”  
(Garante della Privacy)

La sicurezza informatica è un obbligo di legge (Codice della Privacy, di seguito denominato Codice), ma anche una necessità imprescindibile. Una falla che consenta l'accesso ad estranei, un virus, possono infatti paralizzare di colpo l'operatività dell'intero sistema informatico consortile. Allo stesso modo, l'utilizzo sbagliato della posta elettronica, di internet o della strumentazione informatica, può mettere a rischio la sicurezza e l'integrità dei dati del Consorzio, oltre che ridurre o bloccare l'operatività della rete.

Per assicurare un adeguato sistema di protezione dei dati, il Commissario ha definito gli indirizzi sulla base dei quali i dirigenti nominano i responsabili e gli incaricati per il trattamento dei dati, censiscono i trattamenti e le banche dati di propria competenza, ed il Ced effettua un'analisi dei rischi, pianificando le misure necessarie nell'ambito del Documento per la sicurezza informatica da approvarsi entro il 31 marzo di ogni anno. Per completare questo sistema, viene adottato il presente disciplinare, allo scopo di regolare l'uso delle risorse informatiche e telematiche dell'ente.

## **1. OGGETTO E FINALITA'**

Per completare il sistema di protezione e di sicurezza dei dati dell'Ente, il Consorzio adotta il presente Disciplinare che, coerentemente alle linee guida fornite in merito dal Garante della Privacy, e nel rispetto dei diritti dei lavoratori e del diritto alla riservatezza, definisce:

- Le modalità d'uso d'Internet, della posta elettronica, della rete consortile e della strumentazione hardware e software (di seguito denominate nel loro insieme "risorse informatiche") messe a disposizione del personale;
- Le modalità di effettuazione dei controlli e le conseguenze, anche disciplinari, di un utilizzo indebito.

## **2. DESTINATARI**

Il presente Disciplinare si applica ai dirigenti, ai dipendenti, agli stagisti, ai collaboratori (lavoratori con contratto di collaborazione coordinata e continuativa, lavoratori delle cooperative affidatarie di servizi, ecc.), agli amministratori ed in genere a tutti gli utenti autorizzati ad usare le rete consortile e gli strumenti informatici e telematici del Consorzio per lo svolgimento della propria attività lavorativa e istituzionale (di seguito denominati "utenti").

Le prescrizioni del presente Disciplinare integrano e non sostituiscono le istruzioni impartite ai responsabili ed agli incaricati in materia di trattamento dei dati.

Il mancato rispetto delle regole e dei divieti di cui al presente Disciplinare costituisce, per i dipendenti, violazione del Codice di comportamento e determina, nel rispetto dei principi di gradualità e proporzionalità, l'applicazione delle sanzioni disciplinari previste dalle disposizioni di legge e dal Contratto Collettivo Nazionale di Lavoro vigente, fatto salvo comunque il diritto del Consorzio al risarcimento dei danni eventualmente patiti a causa della condotta del lavoratore.

Il mancato rispetto delle regole e dei divieti del presente Disciplinare costituisce, per i collaboratori esterni, violazione degli obblighi discendenti dal rapporto instaurato con l'Amministrazione.

## **3. PRINCIPI GENERALI**

La titolarità delle risorse informatiche è in capo al Consorzio. Tali risorse sono messe a disposizione degli utenti per lo svolgimento dell'attività lavorativa e istituzionale. La dotazione di tali risorse non costituisce titolo per l'acquisizione di alcuni diritti in capo all'utente e può essere ridotta, sospesa o eliminata qualora ne sussistano le motivazioni.

Ogni utilizzo non inerente all'attività lavorativa o istituzionale può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto,

minacce alla sicurezza. E' escluso quindi qualsivoglia uso per scopi privati e personali, ad eccezione dei casi d'urgenza e comunque a condizione che tale uso avvenga in modo non ripetuto o per periodi prolungati.

L'utente è responsabile civilmente e penalmente del corretto uso delle risorse informatiche e del contenuto delle comunicazioni effettuate tramite gli strumenti a disposizione.

Il Consorzio privilegia l'attività di prevenzione rispetto a quella di controllo, indicando, in un'ottica di reciproco affidamento, appropriate misure di tutela e promuovendo misure di autotutela da parte degli utenti, nonché assicurando la massima diffusione del contenuto del presente Disciplinare.

Nello svolgimento dell'attività di monitoraggio e controllo il Consorzio agisce nel rispetto della normativa vigente, con particolare riguardo alla tutela dei diritti dei lavoratori ed alle garanzie in materia di protezione dei dati personali, nell'osservanza dei principi di ragionevolezza, correttezza, trasparenza e proporzionalità.

#### **4. AMMINISTRAZIONE DELLE RISORSE INFORAMTICHE**

Per la gestione delle risorse informatiche dell'Ente sono costituite le seguenti figure:

- 1) Referente informatico interno;
- 2) Referente informatico esterno per l'assistenza hardware e software.

Entrambi i referenti sono nominati con delibera della Deputazione Amministrativa.

Il referente informatico interno svolge le funzioni di gestione delle risorse informatiche del Consorzio e di tutela della sicurezza della rete consortile.

Il referente informatico esterno ha il compito di assicurare l'assistenza hardware e software della rete consortile.

I responsabili di settore possono nominare, nell'ambito del personale assegnato, referenti per lo svolgimento di specifiche attività informatiche concordate con la Direzione che ne informerà i referenti informatici interno/esterno.

#### **5. USO DEL PERSONAL COMPUTER**

L'accesso alla postazione di lavoro è subordinato al corretto inserimento delle credenziali di autenticazione (nome utente e password). La scelta, la modifica e la custodia delle credenziali di autenticazione sono così regolate:

- Al primo accesso alla rete, l'utente ha la responsabilità di cambiare la password assegnatagli dal Referente informatico interno. Tale password non deve essere facilmente riconducibile all'utente (es. il nome o la data di nascita), deve essere composta da almeno otto caratteri ed includere sia cifre che lettere.
- Il sistema, mediante avviso a video, invita l'utente a cambiare la password ogni tre mesi;
- La password è strettamente personale e deve essere debitamente conservata assicurandosi di non divulgarla, fatto salvo quanto più avanti previsto in caso di assenza;
- In caso di dimenticanza, occorre rivolgersi al Referente informatico interno che consentirà l'accesso allo scopo di impostare immediatamente una nuova password.

In caso di allontanamento anche temporaneo dalla postazione di lavoro, l'utente deve attivare il salvaschermo con password o deve bloccare il computer (utilizzando i tasti CTRL+ALT+CANC), per evitare che persone estranee effettuino accessi non autorizzati. Il computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate.

Ciascun utente deve delegare per iscritto un altro lavoratore ad accedere a dati e procedure del proprio computer nel caso in cui, durante la propria assenza, ciò si renda indispensabile ed indifferibile per esclusiva necessità di operatività dal servizio. A tale scopo ogni utente comunica, con modalità che garantiscono la riservatezza, al lavoratore da lui delegato le proprie password avendo cura di ripetere la comunicazione ogni volta che esse vengono cambiate.

Nel caso in cui l'utente non abbia delegato un suo fiduciario e, per garantire l'ordinaria operatività del servizio, sia necessario accedere a informazioni o documenti di lavoro presenti sul computer dell'utente, inclusi i messaggi di posta elettronica, il responsabile del servizio, a cui è assegnato l'utente, può richiedere al Referente informatico interno di accedere alla postazione e/o alla casella di posta elettronica dell'utente assente, mediante variazione della password. Di questo intervento, il responsabile del servizio deve dare comunicazione all'utente.

Per finalità di assistenza, manutenzione e aggiornamento, i referenti informatici interno/esterno possono intervenire sulle postazione direttamente oppure tramite collegamento da remoto.

E' vietato:

- Modificare autonomamente la configurazione del personal computer ed impostare protezioni o password ulteriori per l'accesso alla postazione di lavoro;
- Alterare o disattivare le impostazioni di sicurezza e di riservatezza del sistema operativo, del software di navigazione, del software di posta elettronica e di ogni altro programma installato sulla postazione di lavoro, salvo autorizzazione espressa da parte della Direzione;
- Installare ulteriori programmi sulla postazione di lavoro rispetto a quelli in dotazione, anche se gratuiti, che non siano espressamente autorizzati per scritto dalla Direzione;
- Collegare alla postazione di lavoro dispositivi di memorizzazione (CD, chiavi USB, DVD), senza verificarne previamente l'integrità attraverso il programma antivirus;
- Detenere sulle postazioni di lavoro e/o stampare materiale di contenuto non attinente allo svolgimento dell'attività lavorativa, nonché materiale contrario alla legge o coperto da diritto d'autore, senza in quest'ultimo caso aver attivato i necessari adempimenti di legge.

La Direzione, sentiti i referenti informatici, può in qualsiasi momento procedere alla rimozione di file o applicazioni che riterrà essere pericolosi per la sicurezza, sia sulle stazioni di lavoro, sia sui server di rete.

## **6. USO DI COMPUTER PORTATILI E DISPOSITIVI TEMPORANEAMENTE ASSEGNATI**

L'utente è responsabile del computer portatile e dei dispositivi (macchina fotografica, videoproiettore,...) temporaneamente consegnati dal referente informatico interno, e deve custodirli con diligenza fino alla loro riconsegna.

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

## **7. USO DI INTERNET**

L'accesso a internet costituisce strumento di lavoro ed è consentito per finalità direttamente attinenti o comunque connesso all'esercizio dell'attività lavorativa. E' escluso qualsivoglia uso per scopi personali,

salvo che tale uso sia motivato da ragioni di urgenza o necessità. E' in ogni caso vietato l'uso reiterato e prolungato per fini personali.

Nell'uso di Internet, sono vietate le seguenti attività:

- Scaricare software non necessari all'attività lavorativa o istituzionale e comunque non espressamente autorizzati per scritto dalla Direzione;
- Scaricare file o accedere a video o audio (ad es. ascoltare la radio o guardare filmati) non necessari alla propria attività lavorativa o istituzionale;
- Utilizzare sistemi di chiamata o videochiamata, partecipare a forum, chat, social network e bacheche elettroniche per ragioni non direttamente attinenti all'attività lavorativa svolta;
- Navigare in internet su siti contrari a norma di legge;
- Effettuare transazioni finanziarie e operazioni di remote banking per scopi personali;
- Installare e utilizzare strumenti per lo scambio di dati attraverso internet con metodologia PEER to PEER (es. eMule, kaza, bittorrent, ecc) indipendentemente dal contenuto dei file scambiati;
- Scaricare documenti di grosse dimensioni durante l'orario di apertura al pubblico degli uffici, a causa del rallentamento della connessione internet che può causare.

Al fine di prevenire un utilizzo improprio di internet, sulla base delle istruzioni previste dal presente Disciplinare, i referenti informatici interno/esterno predispongono sistemi di filtri che bloccano determinate operazioni, quali l'accesso a determinati siti (black list) e il download di file o software aventi particolari caratteristiche (quali ad esempio dimensioni o di tipologia di dato).

Qualora i referenti informatici, nell'esercizio delle proprie funzioni, rilevino elementi che possano far pensare ad un utilizzo anomalo di Internet (es. frequente presenza di virus), devono informare la Direzione.

L'utente interessato è informato delle verifiche relative alla pertinenza dei dati di navigazione con l'attività lavorativa e può chiedere di essere ascoltato, nonché di accedere alla documentazione. Se il responsabile del settore, a seguito delle verifiche compiute, ritiene che vi sia stato un utilizzo improprio della navigazione in Internet, o comunque una violazione del presente disciplinare, avvia i procedimenti conseguenti.

## **8. USO DELLE CARTELLE PUBBLICHE**

Le cartelle presenti nel server del Consorzio, articolate secondo la struttura riportata nel prospetto allegato, sono contenitori documentali 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 collocato in questi spazi, nemmeno per brevi periodi.

Su queste cartelle, sono svolte regolari attività di controllo, amministrazione e salvataggio da parte del personale incaricato, che può procedere in qualsiasi momento alla rimozione di file o applicazioni che riterrà essere pericolosi per la sicurezza della rete.

E' assicurato il salvataggio giornaliero dei soli documenti collocati nelle cartelle pubbliche. Il contenuto del personale computer, compresa la posta elettronica, non viene salvato a livello centralizzato.

Con regolare periodicità, l'utente deve pulire i propri archivi cancellando i file obsoleti o inutili e deve evitare un'archiviazione ridondante.

## **9. USO DELLA POSTA ELETTRONICA**

Il Consorzio mette a disposizione di ogni utente il servizio di posta elettronica per fini esclusivamente lavorativi, assegnando una casella istituzionale, contraddistinta dalla presenza del nome di dominio "paduledifucecchio.it".

E' escluso l'uso per scopi privati, ad eccezione dei casi d'urgenza e di necessità e comunque non in modo ripetuto.

Sono disponibili anche liste di distribuzione (mailing list) del personale e degli amministratori del Consorzio, suddivise per categorie o per funzioni, il cui elenco è disponibile nella Intranet consortile.

Solo gli indirizzi dei singoli uffici possono essere comunicati all'esterno, mentre le restanti liste sono adibite esclusivamente alla diffusione interna d'informazioni di servizio di interesse generale.

Per garantire un utilizzo corretto della posta elettronica, è vietato:

- Utilizzare programmi di posta elettronica diversi da quelli installati sulla postazione di lavoro;
- Aprire messaggi di posta o allegati di tipo eseguibile, salvo il caso di certezza assoluta dell'identità del mittente e della sicurezza del messaggio;



- Inviare o memorizzare messaggi di natura oltraggiosa, volgare, diffamatoria e/o discriminatoria e, in ogni caso, contrari a norme di legge o idonei a creare danni al Consorzio o a terzi nonché messaggi tipo "catene di S. Antonio", appelli e petizioni.

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

In caso di assenze programmate dal lavoro (per ferie o per qualsiasi altro motivo) deve essere attivato preventivamente, laddove previsto, il risponditore automatico. Nel messaggio di risposta deve essere indicato il periodo di assenza ed eventualmente l'indirizzo di posta elettronica di un altro utente al quale fare riferimento in caso di comunicazioni urgenti.

In caso di assenza dal lavoro programmata o qualora non sia stato attivato il risponditore automatico, l'utente deve delegare un altro dipendente per la gestione dei messaggi a lui indirizzati.

E' necessario prestare particolare attenzione alla dimensione dei documenti da allegare ai messaggi di posta elettronica, poiché possono rallentare o addirittura bloccare le prestazioni della rete consortile.

Per inviare documenti di dimensione superiori a 2 Mb oppure quando si deve inviare un documento anche di dimensioni inferiori a 2 Mb a numerosi destinatari, gli utenti devono osservare le seguenti regole:

- Se il destinatario è interno al Consorzio, si utilizzano sempre le cartelle di condivisione di file della rete consortile, indicando nel messaggio la collocazione, senza unire gli allegati;
- Se il destinatario è esterno, si comunica questa necessità alla redazione del sito, che provvederà a salvare il documento in un apposito spazio del server web ed a restituire l'indirizzo web dal quale il destinatario potrà scaricare il documento.

Il responsabile del settore, qualora rilevi un utilizzo improprio della posta elettronica da parte di un utente o comunque una violazione al presente disciplinare, ne informa l'utente interessata che potrà chiedere di essere ascoltato e di accedere alla relativa documentazione. A seguito delle verifiche effettuate, il responsabile di settore avvia, se del caso, i procedimenti conseguenti.

## **10. MODALITA' DI ACCESSO ALLA RETE E AI SERVIZI PER GLI UTENTI ESTERNI**

Per essere autorizzati all'uso delle risorse informatiche e dei relativi servizi, è necessario che gli utenti esterni stipulino un'apposita convenzione con il Consorzio.

Il responsabile del trattamento dei dati, comunica ai referenti informatici, anche via e.mail:

- A quali applicazioni il soggetto esterno è abilitato ed il profilo di accesso;
- La data di scadenza della convenzione.

I referenti informatici impostano un periodo massimo di validità corrispondente alla scadenza della convenzione. Scaduto il periodo di validità, delle credenziali dell'utente, se non intervengono ulteriori comunicazioni, saranno automaticamente disabilitate.

## **11. INFORMATIVA**

Il contenuto del presente disciplinare integra l'informativa fornita ai dipendenti e ai collaboratori ai sensi dell'art. 13 del Dlgs 196/2003 (Codice della Privacy).

## **12. DISPOSIZIONI FINALI**

Al presente Disciplinare sarà data la più ampia pubblicità mediante pubblicazione sul sito internet ed affissione in ogni sede di lavoro accessibile ai tutti i dipendenti e collaboratori.