REGOLAMENTO INFORMATICO INTERNO AI FINI PRIVACY

REGOLAMENTO INFORMATICO INTERNO VALIDO AI SENSI DEL D.LG. 196/03 PER FINI FORMATIVI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

UTILIZZO STRUMENTAZIONE HARDWARE E SOFTWARE

1. È fatto divieto installare sulla strumentazione in uso, hardware fisso o removibile (ad esempio chiavette, internet, cellulari, ecc.) qualora ciò non risulti espressamente richiesto ed autorizzato dal Responsabile di Sede o dalla Direzione Generale.
2. L'Azienda si riserva di eliminare qualsiasi elemento hardware fisso o removibile la cui installazione non sia stata appositamente prevista o autorizzata.
3. In caso di allontanamento dalla propria postazione hardware, è fatto obbligo all'utente disconnettere o bloccare la sessione in modo che il proprio profilo non sia accessibile da altri utilizzatori.
4. Sui PC dotati di scheda audio, non è consentito l'ascolto di programmi, files audio o video in streeming, se non a fini prettamente lavorativi.
5. Qualora si rendessero necessarie modifiche alle configurazioni impostate sul PC in uso, occorre effettuarne richiesta tramite helpdesk aziendale.
6. In caso di furto o smarrimento di dispositivi portatili e/o tablet, effettuare una comunicazione tramite helpdesk aziendale all'Ufficio Ced: http://helpdesk.zanardelli.local/
7. I software autorizzati e installati sui dispositivi in uso sono:

3D View
7Zip gestione archivi
Adobe Flash Player 14 ActiveX
Adobe Reader Dc
AutoCAD 2011 - Italiano
Autodesk Design Review 2011
Autodesk Material Library 2011
Autodesk Material Library 2011 Base Image library
Cam Concept Mill/Turn
CCleaner
Cnc Simulator
CodeBlocks
Fanuc 21 Mill/Turn
Firebird 2.1.2.18118
Foxit Reader
Google Chrome
GW3708
GW64-8
GWBUS-VISION
GWCAD

GWCAP
GWENERGY
GWLUX
GWPBT-Q
GWPRICE
GWSoftware Prolite 7.0
Heidenhein TNC 465 Mill
Java
Mach3
Microsoft .NET Framework 4.5.1
Microsoft Office Professional Plus 2013
Microsoft Office Professional Plus 2016
Microsoft Silverlight
Microsoft SQL Server 2008/2014
Mozzilla Firefox
Nblade
Nero Burnin Rom
NetSupport School
Norman Endpoint Protection
Pdf Creator
PDFCreator
PF Sense
Profis
Protocollo GestCfp
Sinumerick 840D Mill/Turn
Sistemi operativi Windows 7/8/10/2003/2008/2012
SketchUp 2015
SolidWorks 2010
TeamSystem Gamma Enterprise
TeamSystem Multi e sue utility
VmWare Esxi
WinNC EMCO
WinNC-Sie840d
WinPLC7 5.042
WinRAR 5.21
WinRAR gestione archivi

ACCESSO ED USO DEI SISTEMI

1. Ogni utente la cui mansione prevede l'accesso a dati personali contenuti nelle cartelle di rete, si connette alla rete tramite autenticazione univoca personale.
2. Ogni utente la cui mansione non prevede l'accesso a dati personali contenuti nelle cartelle di rete, si connette alla rete tramite autenticazione non nominativa (tipicamente legata al corso frequentato).
3. Le credenziali ad autenticazione univoca e personale devono essere richieste mezzo mail o helpdesk dal Responsabile di Sede o dalla Direzione Generale.
4. Le credenziali non nominative legate ai corsi di formazione possono essere richieste mezzo mail o helpdesk dal Responsabile di Sede, dalla Direzione Generale, dai coordinatori didattici o da chi si occupa dell'organizzazione del corso.

5. Le credenziali di autenticazione alla rete devono essere custodite e preservate dalla conoscibilità di soggetti interni e/o esterni all'Azienda.
6. In nessun caso devono essere annotate password personali in chiaro sia su supporto cartaceo che informatico.
7. I requisiti minimi di complessità delle password sulla base della vigente normativa privacy sono:
    a. redazione con caratteri maiuscoli e/o minuscoli;
    b. composizione con inclusione di simboli, numeri, punteggiatura e lettere;
    c. caratteri non inferiori a 8 (ad eccezione dei sistemi operativi che non supportano tali requisiti);
    d. password non agevolmente riconducibile all'identità del soggetto che la gestisce. Pertanto, la password non deve essere basata su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente il soggetto titolare della password stessa.
8. Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere immediatamente a cambiarla e comunicare l'episodio all'Ufficio Ced, al seguente indirizzo mail: assistenzautenti@cfpzanardelli.it.
9. Non debbono essere utilizzate per l'accesso ai portali le opzioni di "compilazione automatica" o remember password, presenti nei browser o in altre applicazioni.
10. L'utente ha l'obbligo di non alterare la funzione "cambio password" dell'accesso alla rete che obbliga a modificare la password con cadenza trimestrale.
11. La scadenza password dei portali utilizzati per scopi lavorativi sono regolate dal gestore del portale stesso.
12. In caso di dispositivi mobili e/o tablet è necessario impostare un codice accesso e/o password per evitare che nessun altro utente possa consultare i dati in esso contenuti in caso di abbandono, furto o smarrimento.

INSTALLAZIONE PROGRAMMI

1. Sul pc in uso non deve essere installato nessun software. Qualsiasi richiesta di installazione deve essere effettuata mediante helpdesk aziendale.
2. Si ricorda all'utilizzatore che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore n. 633/41 come novellata.

UTILIZZO SUPPORTI MAGNETICI E DATI

1. È fatto obbligo conservare, custodire e controllare i supporti informatici removibili contenenti dati, informazioni, notizie o immagini di attinenza aziendale, affinché nessun soggetto terzo ne prenda visione o possesso.
2. Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul pc in uso.
3. Tutti i files di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte dell'ufficio ced tramite richiesta helpdesk.
4. Tutti i file che fanno parte dell'attività lavorativa, devono essere salvati nelle unità di rete messe a disposizione e mai localmente sul pc.
5. Gli accessi alle cartelle di rete o la creazione di cartelle condivise devono essere richieste mezzo mail o helpdesk dal Responsabile di Sede o dalla Direzione Generale.
6. I profili utente al momento della disconnessione vengono salvati sul server di sede.

UTILIZZO RETE INTERNA

1. La rete interna, istituita appositamente per permettere collegamenti funzionali tra utenti che prestano servizio all'interno della struttura lavorativa, non può essere utilizzata per scopi diversi da quelli ai quali è destinata.
2. Qualora nella rete interna debbano circolare dati, notizie ed informazioni aziendali, deve essere premura di ciascun utente preservare gli stessi dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati.

UTILIZZO RETE ESTERNA INTERNET

1. È fatto divieto memorizzare dalla rete documenti, file o dati comunque non attinenti lo svolgimento delle attività aziendali, in particolare:
    a. è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
    b. non è permessa la partecipazione, per motivi non professionali, a Forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames) potendo;
    c. esporre a rischi di sicurezza la rete aziendale.
2. Si rende nota l'attivazione di filtri idonei ad evitare navigazioni in siti non correlati all'attività lavorativa.
   Le categorie bloccate dal sistema sono:

[blk_BL_aggressive]
[blk_BL_alcohol]
[blk_BL_anonvpn]
[blk_BL_costtraps]
[blk_BL_dating]
[blk_BL_drugs]
[blk_BL_dynamic]
[blk_BL_gamble]
[blk_BL_hacking]
[blk_BL_porn]
[blk_BL_redirector]
[blk_BL_sex_lingerie]
[blk_BL_spyware]
[blk_BL_tracker]
[blk_BL_violence]
[blk_BL_warez]
[blk_BL_weapons]

   La black-list con la definizione dei siti viene periodicamente aggiornata dal seguente url http://www.shallalist.de/Downloads/shallalist.tar.gz
3. Si rende noto che l'Azienda ha attivato sistemi di monitoraggio della navigazione aziendale secondo le previsioni di cui al Provvedimento del Garante in materia di trattamento dati personali, Provvedimento del 1 marzo 2007, effettuando monitoraggio generalizzato ed anonimo dei log di connessione individuando per ogni singolo dispositivo i siti visitati con data, ora, dimensione traffico effettuato. A questo proposito verranno forniti alle sedi del CFP Zanardelli dei report che indicano i siti più visitati all'interno di ogni struttura.

4. Gli archivi di log risultanti da questo monitoraggio contengono traccia di ogni operazione di collegamento effettuata dall'interno della rete aziendale verso Internet.
5. Eventuali attivazioni di controlli specifici saranno preventivamente notificate.
6. Nei laboratori non sarà consentito accedere ad alcun tipo di social network.

UTILIZZO FAX

1. Si raccomanda di non lasciare documenti incustoditi presso le postazioni di fax all'atto dell'invio.
2. Qualora l'utente sia prossimo a ricevere atti contenenti dati o informazioni riservate via fax, avrà cura di monitorare la postazione fax e preservare – limitatamente alle oggettive possibilità – la conoscibilità di tali dati o informazioni, da parte di terzi non autorizzati.

UTILIZZO POSTA ELETTRONICA

1. Le caselle di posta elettronica date in uso sono destinate ad un utilizzo di tipo aziendale. Si rappresenta che:
    a. non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita;
    b. non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum, newsletter o mail-list, non attinenti l'attività lavorativa.
2. In caso di assenza protratta per più di cinque giorni lavorativi, sono posti a disposizione apposite funzioni di sistema che consentano di inviare automaticamente messaggi di risposta.
3. È fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza.
4. È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
5. È vietato inviare catene telematiche. Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Ufficio Ced all'indirizzo assistenzautenti@cfpzanardelli.it. Non si devono in alcun caso attivare gli allegati di tali messaggi.
6. Per quanto riguarda i soggetti non dipendenti dell'Azienda, si sottolinea che essere titolare di un indirizzo mail aziendale non comporta alcun rapporto di subordinazione ma si rende necessaria per l'accesso ai servizi aziendali e/o allo svolgimento dell'incarico.

GESTIONE, CONSERVAZIONE E CONTROLLO DEI DATI INFORMATICI

1. È fatto divieto applicare sistemi di crittografia, codificazione e simili ai dati aziendali.
2. È fatto divieto rimuovere dalle cartelle di rete dati utili per l'Azienda alla cessazione del proprio rapporto.

SEGRETO PROFESSIONALE

1. L'utente non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in toto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto dall'Azienda, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi.
2. Gli obblighi del personale previsti in questo capo non termineranno all'atto di cessazione del rapporto di lavoro, se non in riferimento a quelle specifiche parti delle informazioni che il dipendente/collaboratore possa dimostrare che erano già di pubblico dominio al momento della conclusione del rapporto, o che lo sono diventate in seguito per fatto a lui non imputabile.

RISERVATEZZA DEI DATI

1. Premesso che per «Informazioni Riservate» si intendono tutte le informazioni di qualsivoglia natura riferite o apprese in occasione dello svolgimento di mansioni per le quali il soggetto è stato incaricato dall'ente, il dipendente/collaboratore si impegna a considerare le Informazioni Riservate come strettamente private e riservate e ad adottare tutte le misure necessarie per non pregiudicare la riservatezza di tali informazioni.
2. Il dipendente/collaboratore si impegna ad utilizzare le Informazioni Riservate unicamente allo scopo di effettuare lo svolgimento dell'attività cui è preposto e di conseguenza a non usare tali informazioni in alcun modo che arrechi danno all'Azienda, né per alcun altro scopo di qualsiasi natura.
3. Gli impegni di cui al presente capo non proibiscono di comunicare Informazioni Riservate:
    a. alla Direzione Generale, ai soci, avvocati, revisori, banche o altri nostri consulenti ai quali la conoscenza di tali Informazioni è necessaria al fine dell'espletamento di attività funzionali all'Azienda;
    b. soggetti diversi da quelli specificati alla precedente lettera a., qualora ciò sia stato autorizzato dall'Azienda.
4. L'obbligo di riservatezza non opera in caso di Informazioni Riservate:
    a. che al momento in cui vengono rese note siano di pubblico dominio;
    b. che diventino di pubblico dominio dopo essere state rese note per causa non imputabile al dipendente/collaboratore.
5. L'impegno di riservatezza di cui al presente capo si protrarrà anche dopo la cessazione del rapporto di lavoro e sino a quando le informazioni in oggetto non saranno rese di pubblico dominio.

APPLICAZIONE ED INTERPRETAZIONE DEL PRESENTE REGOLAMENTO

1. Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, il personale può rivolgersi all'Ing. Gian Luigi Inversini (ufficiotecnico@cfpzanardelli.it).

DISCIPLINA DEROGHE E MODIFICHE DEL PRESENTE REGOLAMENTO

1. Qualora al presente regolamento l'Azienda intenda apporre modifiche, queste saranno applicate dandone conoscenza immediata al personale.
2. Deroghe o modifiche di uno o più punti del presente regolamento, non rendono invalidi gli altri punti.

Brescia, 24/10/2016

Prot. 1072/A17

Il Direttore Generale
(Ing. Marco Pardo)