UNIPOL GRUPPO FINANZIARIO

MANUALE SULL'UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI

(Per la Sicurezza delle Informazioni)

UNIPOL ASSICURAZIONI · Navale ASSICURAZIONI DAL 1914 · Navale ASSICURAZIONI VITA · UNISALUTE · LINEAR Assicurazioni in Linea · Aurora

1. INTRODUZIONE

1.1. Premessa

Con il presente documento si vogliono fornire, a tutti i Dipendenti ed Utenti dei sistemi informatici (ad eccezione del personale di Agenzia), idonee istruzioni relative alle modalità di utilizzo degli strumenti informatici, anche in base a quanto richiesto dal Codice in materia di protezione dei dati personali emanato con Decreto Legislativo n. 196 del 30 giugno 2003[1] (di seguito Codice Privacy).

Nel Manuale sono contenute istruzioni, indicazioni, raccomandazioni e regole valide per tutte le Società del Gruppo. Per le peculiarità delle singole Società si rimanda a specifici capitoli allegati al presente documento. E' previsto, nel corso del 2008, il raggiungimento di un'uniformità di regole e standard validi per tutti i Dipendenti ed Utenti del Gruppo.

Nello specifico potranno essere successivamente divulgate informazioni più dettagliate relative all'utilizzo delle risorse informatiche, a cura della Direzione Servizi Informatici.

Le linee guida e le istruzioni riguardano:

- Compiti e responsabilità degli Utenti dei Sistemi Informatici
- Norme generali di gestione delle risorse informatiche
- Accesso ai dati e ai sistemi
- Virus e antivirus
- La Posta Elettronica
- Internet

Il mancato rispetto di quanto indicato nel presente manuale costituisce violazione del Regolamento di disciplina e può comportare l'applicazione delle misure disciplinari previste dalla Società.

1.1.1. Distribuzione e Diffusione

Il Manuale, pubblicato sulla Intranet aziendale, è un allegato alla DIS relativa agli <<Adempimenti previsti dal D.Lgs. n°196/03 – Comunicazioni agli incaricati del trattamento, istruzioni, misure di sicurezza ed interventi formativi>>, con la quale tutti i dipendenti sono nominati "Incaricati del Trattamento dei dati personali" come previsto dal Codice Privacy.

1.1.2. Conservazione e Revisione

L'ultima versione del documento é conservata in formato cartaceo dalla funzione Privacy di UGF, che provvede anche a conservarla in forma elettronica su file server.

Il documento sarà revisionato con cadenza annuale e comunque al verificarsi di variazioni normative o modifiche delle architetture dei Sistemi Informatici.

[1] *Il testo completo del Codice è consultabile sulle intranet aziendali delle Società o direttamente sul sito del Garante della Privacy www.garanteprivacy.it.*

2. COMPITI E RESPONSABILITA' DEGLI UTENTI DEI SISTEMI INFORMATICI

L'Utente ha la responsabilità di utilizzare le risorse informatiche, di cui al successivo punto 3, secondo le autorizzazioni che gli sono state assegnate.

Secondo quanto di seguito specificato, al verificarsi di particolari eventi o condizioni possono essere disposti controlli atti a verificare che l'Utente faccia un uso corretto delle risorse assegnategli e delle relative autorizzazioni.

Va infatti sottolineato che:

- l'Utente dei sistemi informatici è tenuto a rispettare le leggi in vigore, ed in particolare la normativa sulla tutela del software (che vieta di copiare software se non espressamente consentito dal contratto di acquisto) ed il Codice Privacy richiamato esplicitamente in precedenza;
- i personal computer, siano essi fissi o mobili, i relativi programmi e/o applicazioni, ivi compresi gli accessi a Internet e le caselle di Posta elettronica, concessi in dotazione ai dipendenti sono beni di proprietà dell'Azienda e costituiscono strumenti di lavoro. Pertanto tali strumenti vanno custoditi in modo appropriato, possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non anche per scopi personali, tanto meno per scopi illeciti e ne debbono essere prontamente segnalati il furto, il danneggiamento e/o lo smarrimento.

Sono da evitare atti o comportamenti contrastanti con le predette indicazioni come, a titolo esemplificativo, quelli di seguito richiamati:

- è assolutamente vietato in Azienda usare e installare programmi non distribuiti da chi ne è preposto ufficialmente;
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non è consentito modificare le configurazioni impostate sul proprio PC;
- non è consentito installare sul proprio PC mezzi di comunicazione propri (come ad esempio i modem, apparati o schede Wi-Fi), salvo esplicita autorizzazione della Direzione Servizi Informatici;
- onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dalla Direzione Servizi Informatici;
- non è consentito scaricare file non aventi alcuna attinenza con la propria prestazione lavorativa;
- tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo antivirus;
- le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi: qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;

- l'Azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza del sistema ovvero acquisita od installata in violazione del presente Manuale;
- non è consentito navigare in siti Internet non attinenti allo svolgimento delle mansioni assegnate, soprattutto laddove la navigazione possa rivelare le opinioni politiche, religiose, sessuali o sindacali del dipendente;
- non è consentito effettuare alcun genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, se non espressamente autorizzati;
- non è consentito scaricare software gratuiti (freeware e/o shareware) prelevati da siti Internet senza la preventiva autorizzazione da parte del competente Servizio aziendale;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- sulla rete internet non è consentito partecipare per motivi non professionali a forum, utilizzare chat line o bacheche elettroniche o registrarsi in guest book, anche utilizzando pseudonimi (nickname);
- non è consentito memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate;
- 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;
- la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, il suo utilizzo va valutato con attenzione in relazione alla riservatezza dei documenti inviati;
- ogni comunicazione esterna, inviata o ricevuta, che abbia contenuti rilevanti o contenga impegni per la Società, che esulano o eccedono dalle proprie autonomie e mansioni**,** deve essere visionata od autorizzata dal diretto responsabile, facendo riferimento per analogia alle procedure in essere per la corrispondenza ordinaria;
- non è consentito utilizzare l'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum o mail-list.

Si rimanda ai capitoli successivi l'approfondimento sulle raccomandazioni qui segnalate.
L'inosservanza delle suddette norme può comportare sanzioni civili e penali nei casi previsti dalla legge, ovvero di tipo disciplinare secondo principi di proporzionalità in relazione alla gravità delle violazioni emerse.

2.1.1. Controlli

In coerenza con quanto previsto dall'art. 4 della legge 300/1970 (Statuto dei lavoratori) ed in applicazione del Provvedimento del Garante per la protezione dei dati personali dell'1 marzo 2007, la Società non effettua alcun tipo di controllo diretto a

distanza sui lavoratori mediante l'utilizzo di apparecchiature e sistemi informatici volti ad una sistematica lettura o registrazione dei messaggi di posta elettronica od alla riproduzione/memorizzazione delle pagine web visualizzate dal lavoratore.
La strumentazione elettronica fornita al lavoratore dall'azienda è destinata ad un utilizzo per esclusivi fini lavorativi; poiché, in caso di violazioni contrattuali e giuridiche sia la Società, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, la Società stessa verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.
Ai fini di assistenza, manutenzione o aggiornamento informatico possono essere effettuati interventi "in remoto" sulla postazione informatica dopo averne dato preventiva informazione all'interessato e solo dietro suo esplicito consenso; in mancanza del consenso si procederà agli indicati interventi alla diretta presenza dell'interessato.

3. NORME GENERALI DI GESTIONE DELLE RISORSE INFORMATICHE

3.1. Premessa

Con il termine "risorse" si intendono tutti i sistemi hardware e software in dotazione agli Utenti utilizzate per l'automazione delle attività di lavoro: personal computer (e accessori), stampanti, scanner, dispositivi mobili (quali Blackberry, palmari, cellulari, schede WIRELESS-UMTS, ecc..) e sistemi/programmi software installati e utilizzati.
Queste risorse hardware e software sono fornite e amministrate dalla Direzione Servizi Informatici e assegnate all'Utente come configurazione standard del posto di lavoro secondo modalità concordate con la Direzione.

3.2. Risorse hardware

3.2.1. Il Personal Computer

Dopo la consegna del personal computer o altro hardware da parte della Direzione Servizi Informatici, l'Utente è responsabile del suo corretto utilizzo e della sua conservazione.
La macchina e le sue principali componenti (monitor, scanner e altro) vengono considerate dotazione dell'Utente e, in quanto tali, gestite a livello di inventario.
Non è ammesso alcuno scambio di risorse hardware o di parti o accessori di esse tra diversi Utenti, se non esplicitamente autorizzato dalla Direzione Servizi Informatici.
In quanto dotazione dell'Utente, in caso di passaggio di quest'ultimo ad una nuova struttura organizzativa nell'azienda e previa comunicazione alla Direzione Servizi Informatici, l'hardware in dotazione viene anch'esso "trasferito" nella nuova destinazione assegnata all'Utente.
Solo il personale preposto della Direzione Servizi Informatici e i tecnici di società terze (questi ultimi su delega della Società a in base ad accordi contrattuali di manutenzione) possono intervenire sulle componenti della macchina.
Nel caso di dimissioni o di assenza prolungata dell'Utente per lunghi periodi (es. in caso di missioni), il responsabile diretto dovrà tempestivamente informare la Direzione Servizi Informatici che provvederà a ritirare la dotazione di risorse informatiche non più utilizzate.

3.2.2. Il personal computer portatile

Il personal computer portatile, qualora autorizzato, è sostitutivo del personal computer da tavolo.
Gli Utenti di personal computer o altri dispositivi elettronici portatili dovranno prestare massima attenzione alla protezione e conservazione di queste risorse loro assegnate. E' in ogni caso opportuno che questi dispositivi non vengano mai lasciati incustoditi; si raccomanda l'utilizzo della catena di sicurezza (se non in dotazione richiederla alla Direzione Servizi Informatici).
Il portatile, se non utilizzato, dovrà essere mantenuto in luogo chiuso e sicuro.
Riportiamo di seguito alcune norme comportamentali :

- In caso di viaggi o spostamenti non consegnare il portatile come bagaglio e custodirlo in modo sicuro assicurandolo alla catena di sicurezza
- Gli aeroporti e i mezzi di trasporto pubblico sono zone esposte a rischio di furto; pertanto prestare la massima attenzione

- Non prestare ad altri il portatile poiché e' destinato esclusivamente ad uso personale
- E' assolutamente sconsigliato lasciarlo in macchina o deporlo nel portabagagli
- Utilizzarlo esclusivamente per gli scopi previsti

Si prevede l'introduzione di accorgimenti per la crittografia dei dati al fine rendere inutilizzabili le informazioni contenute nei dispositivi mobili (PC portatili, cellulari, palmari e Blackberry, CD/DVD, Floppy Disk e memorie USB), in caso di furto o smarrimento.

3.2.3. Cellulare , Palmari e Blackberry

Per questi dispositivi è necessario ossevare le stesse attenzioni comportamentali riservate ai portatili.
In aggiunta è opportuno:

- Proteggere la carta SIM ed i dispositivi con un codice PIN
- Non lasciare mai i dispositivi in macchina od in abiti incustoditi.

3.2.4. CD Floppy Disk e Memorie USB

Tali dispositivi, nel caso contengano dati personali/sensibili, devono essere chiusi in luoghi sicuri.
I CD e floppy disk obsoleti che si intendono inviare al macero dovranno essere preventivamente distrutti o resi quantomeno illeggibili, oppure (ove previsti) riposti negli appositi contenitori "tritadocumenti".
Prestare particolare attenzione alle memorie USB in quanto dispositivi ad alta capacità di memorizzazione e di facile smarrimento.

3.3. Risorse software

3.3.1. Configurazione standard

I personal computer consegnati all'Utente hanno una configurazione software standard. Tale configurazione permette di svolgere tutte le attività ritenute essenziali nei normali processi di lavoro.
Non è ammessa alcuna variazione ad opera dell'Utente della configurazione software standard presente sulle macchine (in allegato la configurazione standard a cui tutti i personal computer di gruppo si uniformeranno).
Per specifiche esigenze di servizio delle Società la configurazione software può essere diversa da quella standard e può essere variata solo su specifico intervento da parte del personale preposto della Direzione Servizi Informatici.
L'Utente non può:

- aggiungere o togliere (installare né disinstallare) software
- modificare impostazioni predefinite che producano conseguenze sull'accesso ai dati e alla rete
- variare qualsiasi opzione di programma che esuli dalla semplice personalizzazione visiva di barre, icone e facilitazioni nell'accesso alle funzioni
- installare programmi di alcun genere, anche se in possesso di regolare licenza a titolo personale
- collegare al Personal Computer qualsivoglia accessorio hardware non fornito o autorizzato dalla Direzione Servizi Informatici

Tale standardizzazione non vuole, in linea di principio, costituire un limite, essendo dettata da una precisa scelta programmatica volta a consegnare all'Utente finale strumenti informatici efficienti, compatibili con la piattaforma generale e con l'architettura dei sistemi, in grado di dialogare correttamente con le altre realtà aziendali e del Gruppo.

3.3.2. Dotazione di Programmi software aggiuntivi

E' politica aziendale rispettare l'etica commerciale e le regole legali in vigore; pertanto non è permesso possedere, senza averne pieno titolo e diritto (es. licenza concessa alla Società), software acquisito dall'esterno per il cui utilizzo possa anche essere previsto un pagamento, ma per il quale non si sia stati esplicitamente autorizzati.

Nel caso esistano particolari o specifiche attività di un Utente/ufficio che possano essere supportate da strumenti software non presenti nella configurazione standard, la Direzione Servizi Informatici, su richiesta dell'Utente e previa autorizzazione del Dirigente Responsabile, valuterà il prodotto più adatto e, verificata la compatibilità con gli standard aziendali, curerà l'installazione del software prescelto.

La fornitura del software (come l'hardware) è di esclusiva competenza della Direzione Servizi Informatici di UGF e il suo utilizzo deve essere fatto nel rispetto delle istruzioni emanate da quest'ultima e delle procedure aziendali.

4. ACCESSO AI DATI E AI SISTEMI

4.1. Identificativo Utente

In base alle norme definite dal Codice Privacy, il sistema informatico deve essere sempre certo dell'identità di chi opera su di esso; pertanto, all'apertura di una sessione di lavoro occorre procedere all'autenticazione dell'Utente da parte dal sistema stesso. L'autenticazione dell'identità avviene mediante l'utilizzo di credenziali, cioè di caratteristiche conosciute o possedute esclusivamente dal singolo Utente.

La credenziale di autenticazione è costituita da un codice identificativo e da una password (parola chiave), che deve essere nota esclusivamente al singolo Utente.

L'accesso ai sistemi avviene in due fasi:

- la prima tramite il sistema Windows installato sui Personal Computer che permette l'accesso alla rete
- la seconda, subordinata alla prima, ai sistemi applicativi HOST/UNIX

All'accensione del PC l'Utente vedrà apparire la finestra di Accesso a Windows che permette di accedere alla rete, ai programmi installati sul PC ed alle risorse condivise assegnate; in una fase successiva è possibile accedere al sistema informatico aziendale su HOST o UNIX .

Di volta in volta, specifiche applicazioni prevedono ulteriori credenziali di accesso in funzione delle mansioni assegnate al singolo Utente come, ad esempio, l'applicativo SERTEL utilizzato nei PC degli Utenti del CALL CENTER.

Il codice di identificazione non può essere assegnato ad altri Utenti, neppure in tempi diversi.

Si ribadisce che è assolutamente vietato:

- l'utilizzo dell'identificativo di altri colleghi
- eseguire scambi di identificativi tra colleghi
- accedere contemporaneamente al sistema da diverse postazioni di lavoro, utilizzando il medesimo codice identificativo personale

4.1.1. Identificativo Utente per l'accesso alla rete

In attesa dell'introduzione di una modalità standard di accesso alla rete per i Dipendenti del Gruppo ed i consulenti esterni, rimandiamo all'allegato di ciascuna Società nel quale sono evidenziate le specifiche istruzioni all'accesso.

4.1.2. Identificativo Utente per l'accesso ad applicazioni e servizi su host

Gli Utenti autorizzati potranno accedere alle applicazioni disponibili sui sistemi Host utilizzando il relativo software di emulazione installato su tutti i personal computer.

4.1.3. Identificativo Utente per l'accesso ad applicazioni e servizi su UNIX

Gli Utenti autorizzati potranno accedere alle applicazioni disponibili sui sistemi UNIX utilizzando un codice identificativo legato alle applicazioni di tale ambiente.

4.1.4. Processo di standardizzazione del codice identificativo

Al termine del processo di unificazione dei sistemi informatici e di definizione degli standard di gruppo attualmente in corso, è previsto che l'accesso al sistema informatico (rete e sistemi applicativi) avvenga tramite un Identificativo "standard" così composto :

AAA	XXXXX

dove

- AAA identifica la Società :
  - UGF=UNIPOLGF, NAU=AURORA, UNP=UNIPOL, NAV=NAVALE, LIN=LINEAR, UNS=UNISALUTE
- XXXXX = numero di matricola

Un esempio: al collega Giovanni Verdi di UGF con matricola 325 verrà assegnato l'identificativo UGF00325.

4.1.5. Modalità di accesso per Esterni/Consulenti

A tendere per tutti i consulenti ed esterni del Gruppo l'accesso al sistema informatico avverrà tramite un Identificativo Utente così composto :

E	S	NNNNNN

dove

E	è fisso e significa ESTERNO	
S	identifica la Società e cioè	G =esterno di UGF, A = esterno Aurora, U = esterno Unipol
		N =esterno di Navale, L = esterno Linear, S = esterno UniSalute
NNNNNN	e' un progressivo numerico assegnato dalla funzione preposta della Direzione Servizi Informatici di UGF	

4.2. Password di accesso

L'accesso al PC, oltre che dal codice identificativo, è garantito da una password con le seguenti caratteristiche e requisiti:

- La password deve essere personale e segreta
- La password non va scritta in posti accessibili agli occhi indiscreti di altri Utenti
- La password scade periodicamente e il sistema ne richiede la modifica forzata almeno ogni 90 giorni
- La nuova password deve essere differente dalle ultime 15 password utilizzate
- Dopo il primo accesso o il reset, la password deve essere cambiata da parte dell'Utente
- Dopo 3 tentativi di accesso con password errata l'Identificativo Utente viene bloccato
- La password deve essere composta da un minimo di otto caratteri; è importante che sia costituita almeno da tre tipi di carattere a scelta fra i caratteri alfabetici, numerici e alcuni simboli speciali
- Non devono essere utilizzati come password nomi propri di persona, nomi comuni o termini che possano in qualche modo essere ricollegati all'Utente in questione
- La password deve essere diversa dall'Identificativo Utente
- Dopo aver inserito la nuova password non sarà possibile cambiarla se non è trascorso un periodo minimo di almeno 1 giorno

L'Utente è direttamente responsabile delle azioni effettuate utilizzando il suo identificativo e deve aver cura di mantenere segrete le password modificandole direttamente qualora egli abbia dei dubbi sulla loro effettiva segretezza.

Come per il PC, anche ogni altro dispositivo hardware (cellulare, palmare, Blackberry, connessione mobile etc.) deve prevedere l'utilizzo di una password ogni volta che viene acceso od attivato dallo stato di stand-by.

4.2.1. Richiesta di cambio della Password (reset)

Il reset della password utente (dimenticata) o il suo eventuale sblocco (dopo alcuni tentativi errati) deve essere richiesto dal Responsabile diretto dell'utente al Servizio dedicato alla riattivazione, secondo le seguenti modalità :

- Tramite e/mail indirizzata alla casella "UGF-BOX SUPPORTO DIREZIONE" , indicando su quale sistema (Windows, Host o altro) occorre riattivare l'accesso e specificando cognome e nome, identificativo, numero di telefono (interno o esterno) dell'utente interessato.
- Tramite l'apertura di un ticket in AHD (per gli utenti che dispongono di tale prodotto)

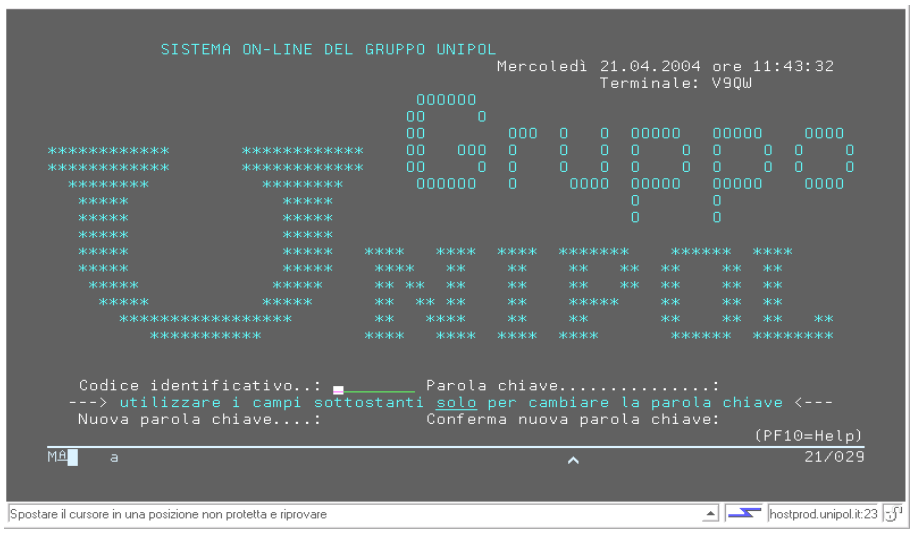
Il Servizio dedicato alla riattivazione provvederà al reset della password mediante una password neutra che verrà comunicata all'Utente; l'Utente, al primo accesso, dovrà immediatamente provvedere al cambio password con una propria parola chiave.

4.2.2. Il cambio della password in ambiente Windows

Su PC Windows è possibile cambiare in qualunque momento la parola chiave utilizzando il bottone "Cambia password…" disponibile sulla finestra che appare quando si premono contemporaneamente i tasti Ctrl-Alt-Canc.

4.2.3. Il cambio della password in ambiente Host

Nella maschera iniziale dell'host è possibile inserire la propria "parola chiave" nel campo "nuova parola chiave"; la digitazione andrà poi replicata nel campo "conferma nuova parola chiave " come mostra la figura.



4.2.4. Il cambio della password in ambiente Unix

Ogni Società con applicazioni in ambiente UNIX fornirà specifiche istruzioni a tutti gli Utenti per il cambio della password in tale ambiente.

4.2.5. Blocco automatico della sessione

La configurazione standard prevede l'attivazione automatica del blocco della sessione (screen saver o salvaschermo) dopo 10 minuti di inattività della macchina.

Lo screen saver ha una duplice funzione. Infatti, da un lato, contribuisce ad aumentare la "vita" del monitor con una generazione casuale di immagini su di esso, dall'altro, permette di impostare un livello di sicurezza per l'accesso alla macchina nel caso di utilizzo in assenza temporanea dell'Utente: dopo l'attivazione automatica dello screen saver il ripristino del regolare funzionamento è infatti subordinato all'introduzione della password.

4.3. Richiesta di abilitazione

In caso di richiesta di nuova abilitazione o di modifica alle abilitazioni esistenti, il Responsabile dell'Utente invia opportuna richiesta scritta alla funzione preposta indicando il tipo di risorsa da abilitare e l'Utente interessato.

In attesa di specifica comunicazione a tutti i Dipendenti del Gruppo, rimangono in vigore le procedure e le disposizioni emanate dalle singole Società.

A breve si provvederà ad emanare apposita procedura (già in vigore presso Aurora) che prevede che il Responsabile dell'Utente invii alla Funzione preposta di UGF apposita richiesta tramite modulo (debitamente compilato in ogni sua parte) secondo le seguenti modalità:

- Via messaggio E/mail allegando il modulo
- Oppure via AHD (per chi dispone del prodotto) allegando il modulo
- Oppure via fax (indicato sul modulo) debitamente firmato dal Responsabile

4.4. Dati personali/sensibili

Nell'ambito della gestione dei profili di autorizzazione e per rispettare quanto richiesto dal "Disciplinare Tecnico in materia di misure minime di Sicurezza" (Allegato B del Codice Privacy), tutte le risorse saranno associate ad uno ed un solo proprietario o Owner.

E' responsabilità dell'Owner

- Assicurare una corretta classificazione in termini di disponibilità e riservatezza (vedi allegato)
- Definire e rivedere periodicamente le restrizioni d'accesso
- Autorizzare gli utenti all'accesso.

4.4.1. I dati sul personal computer

I file contenenti dati personali/sensibili devono essere memorizzati, in via prioritaria, su cartelle definite sui server di rete ed esclusivamente in via temporanea sul disco fisso del personal computer.

4.4.2. Le cartelle memorizzate su File Server

La Direzione Servizi Informatici garantisce il salvataggio ("backup") automatico dei dati/documenti memorizzati sulle cartelle presenti sui server di rete. Il salvataggio viene effettuato giornalmente e, nel caso l'Utente perda o modifichi erroneamente informazioni, sarà possibile il ripristino dei dati/documenti al giorno lavorativo precedente, per un massimo di una settimana.

4.4.3. Riutilizzo di supporti rimovibili.

I supporti rimovibili, come i dischetti floppy, CD/DVD riscrivibili o memorie USB, contenenti dati personali sensibili possono essere riutilizzati da altri incaricati solo se le informazioni contenute al loro interno siano state cancellate.

5. VIRUS E ANTIVIRUS

5.1. Premessa

Sulla infrastruttura di rete (server distribuiti) e sui singoli PC assegnati agli Utenti sono presenti sistemi di prevenzione dagli attacchi dei virus informatici.

In particolare, la configurazione standard dei personal computer prevede un programma di identificazione dei virus che, attivato automaticamente all'avvio del personal computer, è in grado di identificare la presenza di un virus informatico, generando una segnalazione di allarme all'apertura di documenti "infetti".

All'avvio del computer, inoltre, il software antivirus effettua una scansione del disco fisso per verificare l'eventuale presenza di virus. Ogni antivirus presente sui Personal computer viene automaticamente aggiornato.

E' assolutamente vietato:

- Cancellare o rimuovere il software anti-virus dal personal computer
- Inibire la scansione automatica del disco fisso del computer
- Installare software - quali personal firewall o qualsiasi altro software - che possa interferire con l'antivirus ufficiale installato

5.2. Cosa deve fare l'Utente

La probabilità che il proprio PC sia colpito da un virus informatico può essere fortemente ridotta utilizzando i seguenti accorgimenti:

- Cancellare e-mail provenienti da mittenti sconosciuti. Nel caso in cui contengano allegati di qualsiasi natura non aprirli ed avvisare la Direzione Servizi Informatici.
- Non installare mai sul proprio computer programmi passati da amici e/o conoscenti, specialmente da Floppy Disk o da CD
- Mai scaricare e/o copiare programmi da Internet. Nel caso in cui tale operazione fosse necessaria per soddisfare esigenze inerenti la propria attività lavorativa dovrà essere compiuta dal personale preposto della Direzione Servizi Informatici
- Mai lasciare inserito un Floppy Disk, un CD o una unità esterna USB al momento dell'accensione del PC o del suo riavvio

Tutti i casi di sospetto virus devono essere immediatamente comunicati alla Direzione Servizi Informatici.

6. LA POSTA ELETTRONICA

6.1. Premessa

La posta elettronica è uno strumento di comunicazione diffusamente utilizzato, che può però costituire una debolezza del sistema di sicurezza in quanto l'intercettazione di messaggi potrebbe condurre alla diffusione non autorizzata di informazioni riservate.

E' responsabilità del singolo Utente salvaguardare la riservatezza di informazioni e documenti inviati tramite posta elettronica.

In attesa dell'introduzione della crittografia, è responsabilità dell'Utente evitare di utilizzare l'e-mail per messaggi estremamente riservati.

Il servizio di posta elettronica è disponibile anche da internet tramite browser. L'accesso è protetto da un canale crittografato e da user/password.

Deve essere evitato l'utilizzo di tale modalità di accesso alla posta elettronica da locali INTERNET-POINT o altri servizi pubblici.

La *Cassetta Postale* dell'Utente è residente su server centrale ed è indirizzabile:

- dall'interno tramite rubrica da *Cognome Nome*
- dall'esterno, per gli Utenti abilitati, con un indirizzo così composto *nome.cognome@società.it*

La cassetta di posta elettronica ha attualmente una capienza massima di 50 MB.

Raggiunta la soglia di 30 MB il sistema informatico invia un messaggio di avviso di raggiungimento della capienza massima.

Se si superano i 40 MB non si possono più spedire messaggi.

Oltre i 50 MB diventa impossibile sia inoltrare che ricevere messaggi.

Questi limiti potranno variare in funzione di esigenze di governo del sistema di posta. Le variazioni saranno sempre comunicate preventivamente agli Utenti via E/mail dalla Direzione Servizi Informatici.

6.1.1. La firma

Nell'invio di messaggi di posta elettronica usare sempre in calce al messaggio la firma automatica con i riferimenti relativi al proprio ufficio. Esempio:

Nome e Cognome:	Cornelio Nepote
Funzione:	YYYYYYYY
Direzione:	Direzione XXXXX
Società:	Unipol Gruppo Finanziario S.p.A
Indirizzo:	Via Xxxxxxxxx, yy
C.A.P Città Pr Stato:	xxxxx YYYYYY ZZ Italia
Telefono:	Tel. ++39 xx.xxxx.x…x
Cellulare (se in dotazione):	Cell. ++39 xxx. yyyyyy..y
Fax.:	Fax. ++39 xyz. zzzxxxxz
E-mail :	mailto://cornelio.nepote@unipolgf.it
Sito internet:	http://www.unipolgf.it

6.1.2. La clausola di Disclaim

Per tutelarsi da eventuali "accessi indesiderati", qualora non sia automaticamente inserita dal sistema, nei messaggi rivolti verso l'esterno inserire la clausola di "Disclaim" che diffidi dall'usare e dal diffondere informazioni acquisite impropriamente e con la quale si declini ogni responsabilità per eventuali danni derivanti da tali comportamenti illeciti.

Tutte le informazioni contenute in questo messaggio di posta elettronica ed i file ad esso allegati sono riservati e possono essere utilizzati esclusivamente dal destinatario specificato. L'accesso all' e-mail e l'eventuale uso del suo contenuto da parte di un qualsiasi soggetto a ciò non autorizzato sono severamente proibiti.
Nel caso in cui si riceva il messaggio per errore è assolutamente vietato usarlo, copiarlo o comunque divulgarlo mediante comunicazione e/o diffusione e bisogna provvedere sia alla sua cancellazione sia alla distruzione di tutte le copie esistenti.
Ringraziamo anticipatamente per la vostra preziosa collaborazione.

This message is for the designated recipient only and may contain privileged or confidential information. If you have received it in error, please notify the sender immediately and delete the original. Any other use of the email by you is prohibited.
Thank you in advance for your contribution

6.2. Uso corretto

6.2.1. Raccomandazioni

- Non utilizzare la casella di posta elettronica assegnata come archivio. Per messaggi importanti effettuare il salvataggio in cartelle di rete o nel disco fisso del p.c.
- Non usare messaggi a catena, cioè un messaggio divulgato da un soggetto con il solo intento di essere "girato" a tutta una serie di altri riceventi conosciuti e/o sconosciuti
- Per le attività lavorative non utilizzare altri sistemi di e-mail (Hotmail, Libero, etc.) se non quello messo a disposizione dalla Direzione Servizi Informatici
- Non aprire messaggi dalla provenienza e dal contenuto dubbio; segnalare in tal caso il messaggio alla Direzione Servizi Informatici
- Non inoltrare a un indirizzo esterno la posta elettronica in entrata (per esempio: derivazione durante il periodo di vacanze, indirizzo privato e-mail)
- Essere discreti nel diffondere il proprio indirizzo e/mail in modo che non venga inserito in liste massive di mailing
- Per assenze superiori a 2 giorni lavorativi attivare la funzione "FUORI SEDE"
- Non inviare messaggi
    - offensivi, osceni, pornografici o di cattivo gusto
    - contenenti discriminazioni razziali, sessuali, religiose, politiche o sindacali

In caso di specifiche esigenze, concordare preventivamente con la Direzione Servizi Informatici l'invio di messaggi di notevoli dimensioni ad un numero cospicuo di Utenti in modo da minimizzare lo stress sul servizio di posta elettronica. Ogni violazione

determinata da uso improprio della posta elettronica ed avente ripercussioni determinanti sul sistema aziendale sarà sanzionato a norma del Regolamento Disciplinare.

6.2.2. Come creare messaggi standard

Soggetti (mittente/destinatario)

- Evitare che gli elenchi "A" e "CC" siano molto lunghi (è stato fissato un limite di un massimo di 50 indirizzi)

Oggetto:

- L'oggetto deve essere sempre espressamente indicato
- Assicurarsi che la descrizione dell'oggetto sia concisa (40 caratteri al massimo) ed attinente al contenuto della e-mail
- Nella riga dell'oggetto indicare, prima dello stesso, il grado di riservatezza del messaggio (interno, confidenziale, riservato).

Allegati

- Non allegare file a meno che non sia strettamente necessario
- Limitare il numero di file allegati ad un messaggio
- Limitare l'estensione dei file allegati ai messaggi (al massimo 5 MB)
- Procedere sempre ad una loro compressione, verificando a priori che il destinatario sia in grado di decomprimerli
- Qualora si riceva da parte di un Utente sconosciuto un messaggio con un file allegato dal contenuto dubbio NON APRIRLO ma chiedere l'intervento del personale preposto della Direzione Servizi Informatici
- E' vietato inserire allegati la cui estensione del nome è elencata nell'allegato apposito (8.9)

Conclusione del messaggio

- Verificare che venga inclusa sempre la firma, comprensiva dei riferimenti relativi al proprio ufficio.

7. INTERNET

7.1. Accesso ad Internet

La Società ha il compito non solo di incoraggiare ma anche di sostenere, con ogni mezzo, un impiego appropriato di Internet. Le regole previste dalla politica aziendale su Internet devono rivolgersi a tutti coloro ai quali ne viene concesso l'utilizzo, indipendentemente dal fatto che si tratti di personale interno, esterno, consulenti ecc.

Internet è un canale di comunicazione e come tale ha una capacità di servizio limitata. Pertanto un "abuso" di navigazione da parte degli Utenti potrebbe avere effetti collaterali sul sistema di produzione dell'Azienda.

L'abilitazione all'accesso a Internet necessita di apposita autorizzazione inviata da un Dirigente Responsabile alla Funzione preposta dalla Direzione Servizi Informatici di UGF.

In attesa di specifica comunicazione a tutti i Dipendenti del Gruppo, rimangono in vigore le procedure e le disposizioni emanate dalle singole Società.

In caso di mobilità di personale da un'unità ad un'altra l'Utente perde automaticamente i diritti di accesso ad Internet e il nuovo Responsabile, dotato dell'autorizzazione di cui sopra, dovrà farne nuovamente richiesta. Non tutti i dipendenti saranno abilitati a tale servizio che verrà concesso loro solo per situazioni di reale necessità.

In ogni caso, essendo l'accesso ad Internet un ulteriore strumento di lavoro messo a disposizione dalla Società, potrà essere revocato qualora si accerti un protratto e reiterato uso improprio di tale strumento.

Inoltre:

- La navigazione in Internet da una postazione remota di proprietà della Società (vedi accesso remoto) non è consentito. Infatti il PC non sarebbe adeguatamente protetto contro virus, quindi potrebbe "infettarsi" e propagare il virus appena venisse connesso alla rete LAN della Società, prima che i sistemi di difesa della Società possano intervenire a aggiornare l'antivirus del Personal Computer
- E' assolutamente vietato modificare la configurazione predisposta dalla Direzione Servizi Informatici.

7.2. "Download" di software

L'autorizzazione alla consultazione di banche dati su Internet non prevede la possibilità di scaricare ("download") software da siti Internet sul personal computer aziendale.

Gli Utenti che, per esigenze lavorative, abbiano necessità di disporre di versioni dimostrative ("demo") di software, reperibili via Internet, potranno inviare richiesta alla Direzione Servizi Informatici che effettuerà il download del software in maniera sicura, pianificandolo nei momenti di minor traffico di rete.

In ogni caso l'installazione verrà effettuata dalla Direzione Servizi Informatici solo dopo la verifica dei requisiti tecnici e di sicurezza del software.

7.3. Raccomandazioni

Si raccomanda :

- Che l'uso dello strumento sia limitato all'adempimento dell'attività lavorativa
- Che la sicurezza della Società non sia compromessa da usi illegittimi e/o illegali; pertanto è severamente proibito collegarsi e scaricare materiale da siti aventi contenuto illegale, immorale, offensivo, ecc.

- Di non utilizzare gli strumenti messi a disposizione dalla Società per accedere/tentare l'accesso a sistemi esterni superandone, senza autorizzazione, i controlli di sicurezza
- Di non sottoscrivere abbonamenti a pagamento a siti Internet o banche dati informatiche esterne.

L'uso di servizi quali forum, bollettini, ecc. che comportano rischi sul piano legale può compromettere seriamente ed irreparabilmente la reputazione e l'immagine della Società.
Per evitare che le suddette tipologie di danni si concretizzino, gli Utenti devono astenersi - via Internet - dal fornire informazioni

- relative a clienti che potrebbero avvantaggiare la concorrenza
- atte a ledere la credibilità e la reputazione della Società
- che portino i Terzi a conoscenza dei sistemi interni, delle banche dati, delle reti e delle procedure delle quali si avvale la Società.

7.4. Categorie di siti vietati

Nel rispetto delle normative vigenti, è vietato agli Utenti l'accesso a siti riguardanti:

- SESSO e VIOLENZA
- DROGA
- FILE MUSICALI (ES. MP3)
- SCOMMESSE e GIOCHI
- SITI INERENTI LA FRODE INFORMATICA
- WEB CHAT e WEB-BASED EMAIL
- MILITARISMO E ARMI
- RAZZISMO
- RELIGIONE
- ALCOOL e TABACCO
- HOBBIES, RELAZIONI PERSONALI e INCONTRI
- SITI DI CATTIVO GUSTO O SU ARGOMENTI ILLECITI E DISCUTIBILI
- RADIO, TV , FILMATI

L'accesso è da considerarsi potenzialmente pericoloso per la sicurezza aziendale e fonte di rischio di saturazione del canale trasmissivo.
Per meglio presidiare la sicurezza dei sistemi e degli impianti, a breve verrà adottato un sistema centralizzato di filtraggio, volto a prevenire la possibilità di accesso a siti riconducibili alle predette categorie.

7.5. Accesso alla rete da remoto

Per ragioni di servizio è possibile connettersi da remoto alla rete aziendale solo col personal computer aziendale tramite modem (collegato ad una normale presa telefonica) con accesso RAS (Remote Access Service) o tramite Internet.
Quest'ultimo può avvenire con rete ADSL, Fibra Ottica o scheda Wireless (es. UMTS).

La connessione, creata sui canali precedentemente indicati, è "sicura" in quanto realizzata attraverso una VPN (Virtual Private Network in cui i dati viaggiano crittografati in un canale virtuale protetto)

L'abilitazione all'utilizzo necessita di apposita autorizzazione firmata da un Responsabile di Direzione o di Funzione di Staff e inviata ad una Funzione preposta dalla Direzione Servizi Informatici di UGF.

In attesa di specifica comunicazione a tutti i Dipendenti del Gruppo, rimangono in vigore le procedure e le disposizioni emanate dalle singole Società.

Le schede WIRELESS (es. UMTS HSDPA) sono assegnate al solo personale dirigente. Eventuali assegnazioni ad altri collaboratori debbono essere richieste dal Dirigente Responsabile, motivandone l'esigenza e comunque solo per una attività progettuale ovvero con indicazione della data di restituzione della scheda.

In caso di mobilità di personale da un'unità ad un'altra l'Utente perde automaticamente i diritti di accesso remoto e il nuovo Responsabile, munito dell'autorizzazione di cui sopra, dovrà farne nuovamente richiesta.

Per ragioni di sicurezza non è consentito il collegamento simultaneo alla rete via LAN e tramite accesso remoto.

8. ALLEGATI

8.1. ALLEGATO - Modalità di accesso per Utenti Aurora o UGF provenienti da Aurora

L'accesso alla rete avviene tramite un Identificativo Utente così composto :

AURXXXXX

dove

XXXXX = numero di matricola

In casi particolari e per dimostrate esigenze di servizio può essere assegnata un doppio identificativo così composto:

AU2XXXXX

dove

XXXXX = numero di matricola

8.2. ALLEGATO - Modalità di accesso per Utenti Unipol o UGF provenienti da Unipol

L'accesso alla rete avviene tramite un Identificativo Utente così composto :

AAAABBB

dove

AAAA	=	primi quattro caratteri del cognome
BBB	=	primi tre caratteri del nome

Nei casi in cui questa regola non individui univocamente un Utente, si utilizzano 5 caratteri del cognome e 2 del nome oppure l'intero cognome.

8.3. ALLEGATO - Modalità di accesso per Utenti Linear o UGF provenienti da Linear

L'accesso alla rete avviene tramite un Identificativo Utente così composto :

AAAABBB

dove

AAAA	=	primi quattro caratteri del cognome
BBB	=	primi tre caratteri del nome

8.4. ALLEGATO - Modalità di accesso per Utenti Navale o UGF provenienti da Navale

L'accesso alla rete avviene tramite un Identificativo Utente così composto :

NAVXXXXX

dove

XXXXX = numero progressivo

8.5. ALLEGATO - Modalità di accesso per Utenti Unisalute o UGF provenienti da Unisalute

A ciascun dipendente, incaricato al trattamento, Utente di sistema è assegnato un codice identificativo personale sia per l'ambiente Windows che per l'ambiente di gestione dei sinistri.

Per entrambe i sistemi lo USER-ID è composto in maniera differente per gli Utenti e per gli operatori del CALL CENTER:

- Lo USER-ID è composto dalle prime sette lettere del cognome e la prima lettera del nome; nei casi in cui questa regola non individui univocamente un Utente, si utilizzano combinazioni di lettere del cognome e del nome atte a definire uno USER-ID univoco
- Per gli operatori del CALL CENTER lo USERID è composto dalle prime tre lettere del cognome e la prima lettera del nome; nei casi in cui questa regola non individui univocamente un Utente del sistema, si utilizzano combinazioni di lettere del cognome e del nome atte a definire uno USER-ID univoco.

8.6. ALLEGATO - Classificazione delle risorse

Le risorse vengono classificate in base alla:

- Disponibilità
- Riservatezza rispetto al business
- Riservatezza in base alla Privacy

Classificazione in base alla disponibilità

Al fine di garantire la continuità del business aziendale è necessario stabilire il massimo periodo di indisponibilità di una risorsa.

Esistono quattro livelli di classificazione riguardo alla disponibilità:

A1	Conseguenze accettabili per indisponibilità fino a 7 giorni solari
A2	Conseguenze accettabili per indisponibilità fino a 14 giorni solari
A3	Conseguenze accettabili per indisponibilità fino ad un mese
A4	Conseguenze accettabili anche se non è più possibile recuperare l'informazione

E' estremamente importante associare correttamente la classe di criticità alla risorsa poiché è in base al risultato della classificazione che vengono stabilite le strategie per il BACKUP ed il DISASTER RECOVERY.

Classificazione in base alla 'Confidenzialità' (riservatezza delle informazioni di business)

I livelli di classificazione sono indipendenti dal luogo e dal supporto di memorizzazione.

Si definiscono i seguenti livelli di classificazione:

L1	Informazione strettamente riservata	• Solo poche persone che devono essere identificate nominativamente sono autorizzate a consultarla o modificarla. • In caso di accesso non autorizzato, importanti interessi o azioni dell'azienda possono essere compromessi causando un serio danno personale o finanziario.
L2	Confidenziale	• Solo un gruppo limitato di addetti è autorizzato a consultarla o modificarla. • L'accesso non autorizzato potrebbe ridurre l'efficacia delle normali attività di business o danneggiare l'immagine dell'azienda. Potrebbe essere anche causa di perdite finanziarie.
L3	Interna	• Per solo uso interno: questa informazione è necessaria per le normali attività ed è accessibile a tutto il personale • Basso danno in caso di accesso non autorizzato
L4	Pubblica	• Tutti possono consultarla

L3 è il livello di default a cui appartengono tutte le informazioni aziendali.

Classificazione in base 'Privacy' (riservatezza dei dati personali)

In adempimento al D.Lgs. 196/03 sulla tutela dei dati personali, è prevista la classificazione dei soli dati personali anche in funzione della loro riservatezza.

Secondo la suddetta legge i dati personali sono classificabili in:

P1	Sensibili Giudiziari	Sono quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni ed organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale. Sono i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o)e da r) a u), del D.P.R. 14 novembre 2002, n.313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato
P2	Comuni	Sono i dati personali che non appartengono alla categoria precedente e che sono definiti all'art. 4 del Codice privacy.
P3	Anonimi	Sono i dati che in origine o a seguito di trattamento non possono essere associati ad un interessato identificato o identificabile.

8.7. ALLEGATO - Configurazione standard del software su personal computer

Ogni personal computer da tavolo o portatile, nuovo o riassegnato, viene pre-configurato come segue:

- Sistema operativo: Microsoft Windows XP Professional con impostazioni generali regolate da "group policy"
- Accesso alla rete: Client per Reti Microsoft in combinazione con protocollo Internet (TCP/IP) e Condivisione File e Stampanti per Reti Microsoft; le impostazioni per la connessione sono regolate da "logon script" e "group policy"; il firewall di Windows è disabilitato, ogni utilizzo di personal firewall, anti-spyware, ad-aware e simili è vietato in quanto tali strumenti interferiscono con il normale funzionamento delle porte di comunicazione con l'antivirus centralizzato, i server e l'ActiveDirectory

- Per i soli notebook: accesso remoto controllato, via VPN Cisco Systems, per l'accesso tramite rete privata virtuale con canale crittografato
- Software per produttività d'ufficio: Microsoft Office Professional Edition 2002 o superiore
- Email: Microsoft Outlook 2002 o superiore con servizio di collegamento a Exchange Server
- Antivirus: Symantec Antivirus 10.1 o successivo
- Sistema di software distribution e hardware inventory
- Internet Explorer 6.0 o successivi con connessione LAN via server proxy ed impostazioni di funzionamento e protezione regolate da "group policy", così come l'homepage ("intranet UGF") e i principali siti d'interesse aziendale
- Emulazione terminale 3270: client HOD (Host on Demand)
- Adobe Reader 8 o successive
- Accessori software forniti dal produttore hardware: es. Accessori IBM, HP, ThinkVantage, ecc.
- Eventuali software di gruppo (Sertel, Geac, Giada, Patrimm, Visore, ecc.) sono installati dopo la consegna e subordinatamente all'avvenuta abilitazione dell'Utente

Le versioni dei software installati potranno subire evoluzioni, programmate sia in funzione dell'offerta del mercato, sia in funzione di mutate esigenze interne.

8.8. ALLEGATO - Elenco estensioni di file non trasmissibili via E/mail

*.AD?	*.BAS	*.CHM	*.EXE	*.FXP	*.HLP	*.INF	*.JS?	*.KSH	*.LNK	*.MDA	*.OPS	*.PCD	*.REG	*.SCF	*.URL	*.VB?	*.WS?
*.APP	*.BAT	*.CMD			*.HTA	*.INS				*.MDE		*.PIF		*.SCR		*.VSD	
*.ASP		*.COM				*.ISP				*.MDT		*.PRF		*.SCT		*.VSS	
*.ASX		*.CPL								*.MDW				*.SH?		*.VST	
		*.CRT								*.MDZ						*.VSW	
		*.CSH								*.MSC							
										*.MSI							
										*.MSP							
										*.MST							