

Versione del regolamento Valevole dal	3-0 1.8.2018	Classificazione di riservatezza Titolare Processi interessati Lingue disponibili	interno IT-SR Gestione informatica DE, FR, IT
Divisioni interessate Destinatari specifici / Distribuzione Sostituisce Attribuzione	Infrastruttura, Viaggiatori, Cargo, Immobili, Gruppo LIDI-R A2 Versione del regolamento 2-0 K 030.1		

Istruzione del Gruppo sull'utilizzo- consentito di Internet e dei servizi e programmi di posta elettronica

Elenco delle modifiche	1
1. Aspetti generali	2
1.1. Premesse, obiettivi.....	2
1.2. Ambito di validità.....	2
1.3. Documenti di riferimento e correlati	2
1.4. Termini e abbreviazioni.....	2
2. Misure di sicurezza amministrative	2
3. Utilizzo di Internet per scopi privati e di lavoro	2
3.1. Accesso a siti Internet per scopi di lavoro	2
3.2. Accesso a siti Internet per scopi privati.....	3
3.3. Controllo dell'utilizzo consentito di Internet	4
3.4. Impedimento tecnico di accesso a determinati contenuti Internet.....	4
3.5. Download di software da Internet e installazione locale dello stesso.....	4
3.6. Rompere le connessioni https crittografate (intercettazione SSL)	5
4. Utilizzo di servizi e di programmi di posta elettronica	5
5. Sanzioni	5
6. Rapporto con direttive e istruzioni	6

Elenco delle modifiche

Versione	Capitolo	Modifica
3-0	3.6	Descrizione del intercettazione SSL
2-0	Tutti	Acquisizione dell'istruzione nel modello corrente del regolamento. Passaggio da K-IT a IT.

1. Aspetti generali

1.1. Premesse, obiettivi

La presente istruzione disciplina il tipo di utilizzo consentito di Internet, dei servizi e programmi di posta elettronica (come in particolare Outlook/Exchange, servizi di posta elettronica via Internet gratuiti, servizi messenger o Outlook) da parte di persone fisiche che possono utilizzare Internet, servizi /o programmi di posta elettronica per mezzo di un accesso locale o remoto alla rete di comunicazione dati delle FFS.

1.2. Ambito di validità

L'istruzione è vincolante per i lavoratori delle FFS nonché di FFS Cargo. Essa è tuttavia vincolante anche per i collaboratori di altre persone giuridiche, nella misura in cui dette persone giuridiche mettono a disposizione dei loro collaboratori le possibilità tecniche indicate nel capoverso precedente, nonché per collaboratori esterni incaricati delle FFS, di FFS Cargo e di altre persone giuridiche che dispongono delle possibilità tecniche indicate nel capoverso precedente.

Tutte le persone fisiche soggette alle disposizioni della presente istruzione sono di seguito denominate «utenti» e la forma maschile include generalmente anche le rappresentanti del genere femminile a scopo di una migliore leggibilità.

1.3. Documenti di riferimento e correlati

K 030.1 «Manuale Security FFS»

1.4. Termini e abbreviazioni

2. Misure di sicurezza amministrative

- 2.1 Il diretto superiore fa in modo, nei confronti degli utenti suoi sottoposti, che questi ultimi siano informati sull'esistenza e sulle disposizioni centrali della presente istruzione [compresa la relativa direttiva sull'utilizzo consentito di Internet, dei programmi e dei servizi di posta elettronica e sull'uso di hardware e software informatici (R Z 400.5 di seguito denominata «direttiva»)]. Il superiore fa presente che l'istruzione, unitamente alla relativa direttiva, può essere visionata e scaricata in qualsiasi momento dall'Intranet delle FFS, nella rubrica Regolamenti FFS.
- 2.2 FFS SA impegnerà con adeguati provvedimenti le altre persone giuridiche di cui al punto 1, capoverso 2 della presente direttiva (ad es. Securitrans ecc.) ad applicare la presente istruzione anche ai relativi collaboratori.

3. Utilizzo di Internet per scopi privati e di lavoro

3.1. Accesso a siti Internet per scopi di lavoro

- 3.1.1 L'utilizzo di Internet per scopi di lavoro da parte dell'utente è ammesso, fatto salvo quanto indicato al punto 3.1.2.

3.1.2 Non è tuttavia consentito:

Aprire siti Internet dei quali l'utente sa, o perlomeno dovrebbe sapere, che presentano contenuti contrari alla legge o alla decenza (in particolare siti con contenuti sessisti, razzisti, estremistici, pornografici, contrari all'etica o diffamatori). Detti contenuti non devono essere né salvati né (in alcun modo) inoltrati a terzi. Nel caso in cui un sito del genere venga aperto per errore, deve essere immediatamente chiuso (senza copiarne o inoltrarne il contenuto).

3.1.3 La direttiva relativa alla presente istruzione può disciplinare l'uso di Internet per transazioni finanziarie nonché per ordinazioni/assegnazione di incarichi per mezzo di carte di credito. La direttiva può inoltre contenere disposizioni relative alla divulgazione di dati sensibili via Internet.

3.2. Accesso a siti Internet per scopi privati

3.2.1 L'accesso a siti Internet per scopi privati da parte dell'utente è consentito nella misura in cui l'accesso sia limitato ad un arco di tempo ridotto. Sono fatte salve le disposizioni del punto 3.1.2 della presente direttiva, che devono essere rispettate anche in caso di utilizzo privato di Internet.

Se gli accessi ai siti Internet consentiti compromettono la disponibilità della rete FFS, il CISO può disporre il blocco dei corrispondenti link.

3.2.2 Tuttavia, se il diretto superiore dell'utente ha un giustificato sospetto o addirittura la certezza che l'accesso a siti Internet consentiti vada al di là della misura ammessa o che il suo sottoposto apra o aprirà siti che non è consentito aprire (cfr. punto 3.1.2), egli ha facoltà di limitare o addirittura di proibire l'utilizzo privato di Internet da parte dell'utente. Questo provvedimento deve tuttavia sempre essere proporzionato. Sono fatte salve le sanzioni di cui al punto 5 della presente istruzione.

L'accesso a Internet può essere interrotto o proibito nell'ambito delle istruzioni di lavoro interne a un reparto, anche quando è proporzionato.

La proporzione è data per esempio dai casi in cui non è necessario alcun accesso a Internet per scopi di lavoro e/o al personale sono affidate funzioni di sorveglianza.

3.3. Controllo dell'utilizzo consentito di Internet

- 3.3.1. L'unità organizzativa IT-Security & Risk Management delle FFS (di seguito abbreviata in «IT-SR») esegue controlli anonimi a campione dei protocolli d'utilizzazione d'Internet in base a orari definiti e per una durata limitata per verificare l'eventuale violazione del punto 3.1.2 della presente istruzione aziendale.

Nel caso in cui si constati un abuso, è possibile eseguire un'analisi del protocollo d'utilizzazione riferito alla persona. Il risultato dell'analisi riferita alla persona deve essere comunicato da IT Sec & Risk al diretto superiore della persona colpevole nonché alla Direzione Human Resources della divisione/del settore centrale per cui lavora la persona colpevole. Il diretto superiore prende le necessarie misure di condotta. I responsabili del personale assegnati sono a disposizione del superiore per assistenza e consulenza.

- 3.3.2. Nell'ambito dei propri controlli, IT-SR deve attenersi alle disposizioni correnti della «Guida relativa alla sorveglianza dell'utilizzazione di Internet e della posta elettronica sul posto di lavoro» dell'Incaricato federale della protezione dei dati.

Non possono essere applicati sistemi di controllo e supervisione volti a controllare il comportamento dei lavoratori sul posto di lavoro. In caso di necessità di sistemi di controllo e supervisione per altri motivi, essi devono essere disposti e configurati in modo da non compromettere lo stato di salute e la libertà di movimento dei lavoratori (art. 26 Ordinanza 3 concernente la legge sul lavoro).

- 3.3.3. In caso di dubbio sull'ammissibilità di un controllo, IT-Sec & Risk chiederà preventivamente una consulenza interna FFS.

3.4. Impedimento tecnico di accesso a determinati contenuti Internet

IT-Sec & Risk è autorizzata e tenuta, allo scopo di impedire danni provocati da cause tecniche (ad esempio la contaminazione da parte di virus), ad applicare le misure di protezione tecniche ammesse per legge. Dette misure di protezione vengono regolarmente adeguate allo stato attuale della tecnica. IT-Sec & Risk ha facoltà di rendere tecnicamente impossibile l'accesso a siti Internet che violano le disposizioni del punto 3.1.2 o che potrebbero danneggiare gli interessi o il buon nome del Gruppo FFS.

3.5. Download di software da Internet e installazione locale dello stesso

Non è consentito scaricare software da Internet e successivamente installarlo localmente. Sono fatti salvi i casi in cui il CISO delle FFS abbia autorizzato l'operazione eccezionalmente per indispensabili ragioni di lavoro.

La direttiva relativa alla presente istruzione può contenere ulteriori disposizioni esecutive su questo oggetto della regolamentazione e sul download di codici software.

3.6. Rompere le connessioni https crittografate (intercettazione SSL)

Per rilevare e bloccare virus e malware nel traffico crittografato, le connessioni crittografate (https) sono suddivise da un proxy in avanti e scansionate da un software. Successivamente, il traffico dati viene nuovamente crittografato e consegnato al destinatario. Il traffico Internet decodificato non viene memorizzato né valutato personalmente. Sono inoltre bloccati i siti Web, le applicazioni e i contenuti indesiderati (violenza, razzismo, pornografia, servizi di streaming).

La crittografia delle comunicazioni con il governo federale, con banche e altri fornitori, che presuppongono un maggiore standard di sicurezza (banche, ospedali e assicurazioni sanitarie), non viene interrotta.

Queste regole si applicano anche agli utenti mobili che accedono a Internet in viaggio o a casa.

4. Utilizzo di servizi e di programmi di posta elettronica

- 4.1. È proibito inviare messaggi e-mail (con o senza allegati) con contenuti contrari alla legge o alla decenza, a prescindere dall'uso del servizio o del programma di posta elettronica (ad es. servizi di posta elettronica gratuiti via Internet o Outlook) e dal fatto che si tratti di un messaggio e-mail privato o di lavoro.
- 4.2. È proibito l'uso di servizi messenger e vocali, che non sono stati messi a disposizione dalle FFS (p.es. MSN - Messenger, Skype), nonché l'invio in massa di messaggi elettronici pubblicitari per scopi privati.
- 4.3. In caso di ricevimento di messaggi e-mail da invii in massa di messaggi elettronici non richiesti a scopo pubblicitario, è possibile segnalare il fatto al servizio di assistenza informatica (166) allo scopo di impedire il ricevimento delle suddette e-mail per il futuro.
- 4.4. La direttiva relativa alla presente istruzione può contenere disposizioni integrative sull'utilizzo dei servizi e programmi di posta elettronica.

5. Sanzioni

- 5.1. Le sanzioni in caso di violazione delle disposizioni della presente istruzione, ma in particolare in caso di violazione dei punti 3.1.2 o 4.1 della presente istruzione, da parte di lavoratori delle FFS, di FFS Cargo o lavoratori di un'altra persona giuridica (cfr. punto 1, capoverso 2), si evincono dal rapporto giuridico derivante dal

contratto di lavoro con il datore di lavoro (una flagrante violazione del punto 3.1.2 o 4.1 può portare al licenziamento senza preavviso).

- 5.2. Le sanzioni possono essere imposte solo se vi è certezza sull'identità del lavoratore colpevole. Le sanzioni devono sempre essere proporzionate. In presenza di un comportamento passibile di punizione, l'ufficio legale di competenza, insieme al responsabile dell'unità organizzativa della persona colpevole, decide se presentare denuncia.
- 5.3. Se un collaboratore di un'altra persona giuridica (ai sensi del punto 1, capoverso 2 della presente istruzione) o un collaboratore esterno incaricato delle FFS, di FFS Cargo o di un'altra persona giuridica ha violato le disposizioni della presente istruzione (compresa la relativa direttiva), il corrispondente datore di lavoro o committente applica le sanzioni proporzionate che ritiene adeguate nei confronti della persona colpevole.
- 5.4. Se la persona colpevole è equivalente dal punto di vista economico all'impresa che ha stipulato un contratto (ad esempio: di servizi informatici) con le FFS, FFS Cargo o un'altra persona giuridica ai sensi del punto 1, capoverso 2 della presente istruzione (ad esempio: ditta individuale o società unipersonale) o se l'impresa si rifiuta di comminare sanzioni proporzionate ai sensi del punto 5.3 nei confronti del proprio impiegato o incaricato colpevole, le FFS, FFS Cargo o l'altra persona giuridica ai sensi del punto 1, capoverso 2 della presente istruzione procedono a verificare la propria futura politica di assegnazione nei confronti di detta impresa e traggono le necessarie conseguenze consentite dalla legge.

6. Rapporto con direttive e istruzioni

Nell'ambito della competenza ad esso delegata con la presente istruzione (cfr. punti 3.1.3, 3.5 ecc. della presente istruzione), IT-Sec & Risk ha facoltà di emanare disposizioni esecutive relative all'utilizzo consentito di Internet, dei programmi e dei servizi di posta elettronica nella «Direttiva sull'utilizzo consentito di Internet, dei servizi e programmi di posta elettronica e sull'uso di hardware e software informatici».

Tuttavia, le disposizioni di detta direttiva non devono essere in contrasto con le disposizioni della presente istruzione. Le modifiche apportate da IT-Sec & Risk alla direttiva, che risultano da una norma di delegazione della presente istruzione, vengono sottoposte a un controllo giuridico preliminare.

IT
F.to Peter Kummer
CIO

IT-SR
F.to Marcus Griesser
CISO