CENTRO AGROALIMENTARE ROMA SCPA

REGOLAMENTO GENERALE PER L'UTILIZZO DELLA RETE TELEMATICA E DEGLI APPARATI

Premessa

Il Centro Agroalimentare Roma C.A.R. S.c.p.A. riconosce il ruolo centrale e strategico della rete informatica come strumento essenziale per il funzionamento, il miglioramento dei servizi offerti e per il perseguimento dei propri obiettivi amministrativi e gestionali.

C.A.R. S.c.p.A., nel favorire l'uso della rete da parte di tutte le sue componenti istituzionali, emana il presente Regolamento che definisce le regole per la gestione e l'utilizzo dei servizi di rete del CAR (Centro Agroalimentare Roma).

Indice

Articolo I. Definizioni 3
Articolo II. Strutture collegate alla rete di trasmissione del CAR 3
Articolo III. Utenti della rete di trasmissione di C.A.R. S.c.p.A. 3
Articolo IV. Utilizzo della rete e regole di accesso 4
Articolo V. Abusi nell'utilizzo della rete 4
Articolo VI. Strutture per la gestione, il controllo 5
Articolo VII. Privacy ed Accesso ai Dati 6
Articolo VIII. Organismo per il coordinamento delle attività tecniche 6
Articolo IX. Struttura della Rete 7
Articolo X. Postazioni di Lavoro 7
Articolo XI. Navigazion Internet e Sicurezza PDL e Apparati Mobile 8
Articolo XII. Backup e Recovery 8
Articolo XIII. Apparati Informatici e Telematici 10
Articolo XIV. Attuazione e variazioni 11

Articolo I. Definizioni

1. La rete di trasmissione dati del CAR rappresenta lo strumento di collegamento delle risorse informatiche distribuite nel campus, aderenti agli standard[1], connesse ai sistemi informativi, ai sistemi fonia ed alla rete internazionale Internet;
2. C.A.R. S.c.p.A. sviluppa e gestisce la rete di trasmissione per le strutture amministrative e gestionali. Per "strutture" si intendono tutti gli stabili e le aree interne al campus del CAR;
3. Sulla rete trasmissione dati del CAR vengono erogati i servizi ai dipendenti di C.A.R. S.c.p.A. ed a tutte le aziende interne al campus (fonia e dati); inoltre, viene utilizzata per tutti i servizi interni (sicurezza, manutenzione, videosorveglianza, rete elettrica, ecc.); l'utilizzo della rete è regolato dagli articoli seguenti e dalle decisioni degli Organi di Gestione, adottate in conformità al presente regolamento e nel rispetto delle norme di legge vigenti.

Articolo II. Strutture collegate alla rete di trasmissione del CAR

Sono collegate alla rete di trasmissione del CAR:

1. Strutture interne, amministrative e gestionali di C.A.R. S.c.p.A., nel rispetto del presente regolamento;
2. Soggetti partecipati da C.A.R. S.c.p.A. richiedenti il collegamento, nel rispetto del presente regolamento;
3. Enti esterni a C.A.R. S.c.p.A.. Le modalità di connessione saranno disciplinate da una convenzione, sottoscritta tra le parti ed approvata dalla Direzione di C.A.R. S.c.p.A., comprovante la collaborazione e l'utilità del collegamento. Gli enti esterni non potranno accedere alla rete del CAR se non preventivamente autorizzati e collegati dal settore preposto.

Articolo III. Utenti della rete di trasmissione di C.A.R. S.c.p.A.

Possono avere accesso alla rete di trasmissione del CAR per scopi amministrativo-gestionali, compatibilmente con le risorse disponibili:

1. Il personale C.A.R. S.c.p.A. e le aziende esterne;
2. I consulenti a contratto, i consulenti visitatori, i collaboratori esterni impegnati nelle attività istituzionali svolte da C.A.R. S.c.p.A., per il periodo di tempo

necessario all'espletamento dei loro compiti all'interno del CAR, previa autorizzazione del settore preposto;

3. Le Organizzazioni Sindacali Locali riconosciute che ne facciano domanda tramite il rappresentante dell'Organizzazione Sindacale Locale che si renda responsabile dell'utilizzo della connessione e/o della casella di posta elettronica;

4. Ogni altra categoria di persone autorizzata dalla Direzione di C.A.R. S.c.p.A., che determinerà tramite l'Ufficio ICT le regole per l'autorizzazione.

Articolo IV. Utilizzo della rete e regole di accesso

1. Qualsiasi accesso alla rete deve essere associato ad una persona fisica, la cui identità dovrà essere documentata. Alla predetta persona fisica devono essere riconducibili le attività svolte utilizzando il codice utente (username di accesso), il sistema personale, il sistema server, l'accesso remoto, l'indirizzo TCP/IP;

2. La richiesta di accesso comporta l'esplicita accettazione delle norme, del presente regolamento, nonché la totale assunzione di responsabilità delle attività svolte tramite la rete. L'uso della rete è in ogni caso soggetto alle norme di legge vigenti;

3. La rete trasmissione di C.A.R. S.c.p.A. può essere utilizzata esclusivamente per l'attività strumentale e di gestione del campus CAR;

4. Ogni utente della rete sarà identificato e sarà tenuto ad adottare le necessarie misure per non interferire con il corretto funzionamento delle comunicazioni, per garantire l'integrità dei sistemi e l'accesso alle risorse da parte degli altri utenti ed evitare che le attività svolte producano disturbo o danni agli altri utenti. Ogni illecito o abuso riscontrato sarà oggetto di successivi provvedimenti sanzionatori;

5. In casi di interventi tecnici urgenti ed improcrastinabili, le connessioni alla rete potranno essere distaccate senza preavviso.

Articolo V. Abusi nell'utilizzo della rete

Costituisce abuso nell'utilizzo della rete trasmissione del CAR:

1. Qualsiasi atto che possa compromettere la sicurezza delle risorse informatiche e la riservatezza delle informazioni di C.A.R. S.c.p.A. o di altri Enti, fruibili attraverso la rete telematica;

2. L'accesso, l'utilizzazione, la distruzione, l'alterazione o la disabilitazione non autorizzata di risorse informatiche, anche per mezzo di chiavi di accesso

(password, badge, ecc.) rese disponibili ad altri soggetti, nonché l'abbandono senza custodia di stazioni di lavoro già connesse a risorse informatiche riservate;

3. La duplicazione, l'archiviazione e l'uso di software su qualsiasi risorsa informatica di C.A.R. S.c.p.A. in violazione a disposizioni contrattuali;
4. L'utilizzazione per scopi d'interesse esclusivamente privato di qualsiasi risorsa informatica di C.A.R. S.c.p.A.;
5. Qualsiasi atto che, tramite la rete telematica del CAR, possa recare disturbo o danni a terzi;
6. L'uso di dati o di altre risorse informatiche per scopi non consentiti dalle norme di legge vigenti o in contrasto con quanto disciplinato nel presente regolamento.

L'uso personale della rete è tollerato purché:

1. non sia a detrimento dei compiti istituzionali;
2. non costituisca un carico avvertibile per la rete;
3. non costituisca un'attività commerciale o comunque con profitto;
4. non sia offensiva;
5. non violi le norme e le leggi in vigore.

In caso di abuso, secondo la gravità del medesimo e fatte salve le ulteriori conseguenze di natura penale, civile ed amministrativa, gli organi responsabili delle risorse informatiche potranno adottare provvedimenti che ne limiteranno l'uso.

L'inosservanza del presente regolamento o, in ogni caso, l'adozione di comportamenti che possano compromettere il funzionamento della rete, saranno segnalati all'utente che sarà richiamato al rispetto delle condizioni d'uso. Nel caso di abusi che rientrino nei punti del presente articolo saranno adottati i necessari provvedimenti urgenti, incluso il temporaneo distacco o la revoca dell'accesso alla rete dell'utente. Qualora il comportamento dell'utente violi le norme di legge e/o causi danni di qualunque natura (economici, d'immagine, violazione della privacy, ecc.) potranno essere adottati provvedimenti disciplinari, amministrativi o legali.

Articolo VI. Strutture per la gestione, il controllo

All'Ufficio ICT sono demandate l'applicazione delle regole tecniche di gestione della rete e la verifica dell'osservanza del presente regolamento. L'Ufficio ICT ha il compito di pianificare, sviluppare, monitorare le infrastrutture di rete che collegano le strutture del campus CAR. L'Ufficio ICT ha il compito di curare il mantenimento e lo sviluppo delle reti informatiche, nonché di monitorare il funzionamento delle infrastrutture delle reti principali. In caso di comprovati e gravi abusi, ed ha il compito

di sottoporre l'evento al Responsabile dell'Ufficio ed al Responsabile della Privacy, di cui al successivo articolo, per l'individuazione di eventuali provvedimenti sanzionatori.

Articolo VII. Privacy ed Accesso ai Dati

La Sicurezza e la Privacy sono gestite tramite suddivisione degli account autorizzati ad operare come amministratori sulla rete, nel rispetto della normativa vigente.[2]

E' presente un account 'administrator', autorizzato ad operare sulle macchine come utente amministratore, normalmente non utilizzato per motivi di sicurezza. L'utente operativo utilizzato ed autorizzato ad operare come amministratore è l'utente 'ced'. Tali account sono autorizzati e creati per operare esclusivamente sulla rete e sugli apparati di C.A.R. S.c.p.A..

L'accesso e la gestione sugli apparati della rete del Campus è effettuata tramite gli account 'cisco' e nativi del vendor Cisco, assegnati al presidio esterno della rete.

L'utente di controllo e supervisione è nominativo e corrisponde al Responsabile ICT, il quale è autorizzato all'accesso ai log del Controller di Dominio e di Rete.

L'accesso ai Dati delle cartelle personali dei Dipendenti è subordinato alle policy di sicurezza di accesso delle cartelle e file, gestite dal File Server (Controller di Dominio). Ogni cartella è pertanto accessibile solo dal relativo account assegnato all'utente. La proprietà della cartella rimane dell'utente 'administrator', il quale è autorizzato per gli ovvi motivi tecnici, alla gestione della stessa.

Articolo VIII. Organismo per il coordinamento delle attività tecniche

Il Responsabile dell'Ufficio ICT, quale supervisore con funzioni di indirizzo, controllo e coordinamento su tutte le attività connesse alle infrastrutture ed ai servizi informatici relativi della rete CAR, si occuperà di:

- coordinare l'Ufficio ICT per quanto attiene le attività inerenti la gestione e lo sviluppo della rete trasmissione di C.A.R. S.c.p.A. e di intraprendere eventuali piani di sviluppo;
- individuare i provvedimenti sanzionatori da proporre agli Organi di Gestione, definendo le azioni tecniche da intraprendere nei casi di gravi abusi.

Articolo IX. Struttura della Rete

La struttura della rete del CAR è definibile come una doppia stella ridondata. Agli apparati di rete di Core e di Distribuzione sono collegati tutti gli strumenti aziendali e postazioni di lavoro. Sono inclusi negli apparati anche gli Access Point Wi-Fi e qualsiasi altro apparato riconducibile e collegabile con la rete Ethernet del CAR.La rete interna di C.A.R. S.c.p.A. è strutturata tramite server dedicati ai servizi aziendali (Autenticazione, Contabilità, Accessi, Sito Web, ecc.) ai quali sono connessi, tramite gli switch di rete, le Postazioni di Lavoro (PDL).

Articolo X. Postazioni di Lavoro

L'accesso alle PDL è vincolato all'inserimento di un Account e password, gestite dal sistema centrale di Active Directory, e rilasciate su autorizzazione dei Responsabili d'Ufficio. Nello specchietto di seguito riportato si riporta l'estratto delle policy applicate agli Account di accesso:

Account Policies

Policies		Settings
Password Policy	Enforce password history	1 passwords remembered
	Maximum password age	60 days
	Minimum password age	0 days
	Minimum password length	6 characters
	Password must meet complexity requirements	Disabled
	Store passwords using reversible encryption	Disabled
Account Lockout	Account lockout duration	15 minutes
	Account lockout threshold	10 invalid logon attempts
	Reset account lockout counter after	15 minutes

Le PDL sono sotto la responsabilità degli utenti che vi accedono. Da ogni PDL è possibile accedervi con qualsiasi Account. E', pertanto, fatto obbligo agli utilizzatori disconnettere il proprio Account alla fine di una sessione di lavoro, bloccare la postazione in caso di allontanamento temporaneo (tramite la pressione della sequenza Ctrl+Alt+Canc) e spegnimento della PDL al termine della giornata lavorativa.

Sono esclusi da tale obbligo gli apparati mobile che sono assegnati personalmente.

Articolo XI. Navigazion Internet e Sicurezza PDL e Apparati Mobile

La navigazione verso Internet delle PDL è regolata da policy di sicurezza e protezione che impediscono, tramite profilazione degli account, l'accesso ai siti rientranti nelle seguenti categorie:

Adult Material	Productivity
Bandwidth	Security
Drugs	Social Web - Facebook
Extended Protection	Social Web - Twitter
Gambling	Social Web - Various
Illegal or Questionable	Social Web - YouTube
Information Technology	Society and Lifestyles
Internet Communication	Tasteless
Intolerance	Violence
Militancy and Extremist	Weapons

Eventuali autorizzazioni diverse, dovranno essere autorizzate ufficialmente dal Direttore Generale e/o Direttore Operativo.

Gli apparati mobile non sono protetti dalla navigazione internet e l'uso corretto è rimandato alla responsabilità dei singoli utilizzatori.

La sicurezza generica delle PDL e degli apparti mobile è effettuata tramite un sistema Antivirus centralizzato che mantiene aggiornato e controlla costantemente la presenza di malware sugli apparati.

Articolo XII. Backup e Recovery

I Server ed i dati conservati nello Storage di Domino, sono replicati e conservati su più sistemi di Backup, NAS ed a nastro, presso il Centro Ingress, dove è realizzata una seconda sala CED dedicata alla ridondanza dei servizi ed al Backup.

Le policy applicate e i backup effettuati sono inicati nella tabella di seguito riportata:

Backup						
	Server	***Tipo***	***Dati***	***Schedulato***		***Conservato***
Symantec Backup Exec 2012 (Appliance)	SRV-Dominio01	Full	System State E:*.*	Sabato	14:00	8 Settimane
		Incremental	System State E:*.*	Lun. - Ven.	13:00	8 Settimane
		Incremental	System State E:*.*	Lun. - Ven.	19:00	8 Settimane
	SRV-Dominio02	Full	System State C:\Ced*.* C:\Ced_Servizio*.*	Mercoledì	11:00	8 Settimane
		Incremental	System State C:\Ced*.* C:\Ced_Servizio*.*	Lun. - Mar. Gio. - Ven.	11:00	8 Settimane
	SRV-Mdaemon	Full	System State C:\Mdaemon*.*	Domenica	13:00	8 Settimane
		Incremental	System State C:\Mdaemon*.*	Lun. - Sab.	13:00	8 Settimane
		Incremental	System State C:\Mdaemon*.*	Lun. - Sab.	19:00	8 Settimane
	SRV-Symantec	Full	C:\Drscripts*.* C:\Program Files\Symantec\Backup Exec\PrepareBEDBRecovery.bat C:\Program Files\Symantec\BEAppliance\Scripts\hostmgt.pl D:\BackupExec\BEDB\BEDB.bak	Lun. - Dom.	8:15	2 Settimane
	SRV-Triton	Full	System State MS SQL Server	Lunedì alterni	7:00	4 Settimane
	SRV-Zucchetti	Full	System State MS SQL Server	Lun. - Sab.	4:00	8 Settimane
		TX Log Incremental	System State MS SQL Server	Sabato	11:00	8 Settimane
	VMWare-Zucchetti	Full	SRV-Zucchetti Zuccapps	Domeniche alterne	14:00	4 Settimane
		Full	SRV-Zucchetti		14:00	4 Settimane

			Zuccapps	Domenich e alterne		
Symantec Backup Exec 2010 R3	***Server***	***Tipo***	***Dati***	***Schedulato***		***Conservato***
	Sigla	Full	Oracle Server	Lun. - Dom.	23:00	8 Settimane
		Full	C:\BKSIGLA\Batch*.*	Domenica	06:30	8 Settimane
	Ares-Server	Full	Oracle Server	Lun. - Dom.	23:00	8 Settimane
		Full	C:\Documents and Settings\Administrator\Desktop\BAT_Backup*.* D:\Backup_oracle*.*	Domenica	6:30	8 Settimane
	SRV-Backup	Incremental	E:\BackupSito*.*	Mercoledì	04:20	8 Settimane

Articolo XIII. Apparati Informatici e Telematici

Gli apparati informatici e telematici di C.A.R. S.c.p.A., quali, Personal Computer, Notebook, Cellulari e Smartphone, SIM, Apparati di connessione remota, ecc., saranno forniti al personale quali strumenti di lavoro in relazione a quanto disposto dalla Direzione di C.A.R. S.c.p.A.. Tali strumenti dovranno essere utilizzati e conservati prestando la massima cura e ricordando che sono di proprietà aziendale. Gli strumenti forniti saranno richiesti dai Responsabili di Area e saranno calibrati secondo modalità tecniche, stabilite dall'Ufficio ICT, in funzione della destinazione d'uso e delle attività svolte dal dipendente a cui andranno fornite ed autorizzati dal Direttore Operativo e/o Direttore Generale.

La sostituzione di tali apparati verrà effettuata per valide motivazioni esclusivamente tecniche quali, in maniera non esaustiva, guasti, variate esigenze di destinazione che necessitino di apparati totalmente diversi, obsolescenza. Nello specifico l'obsolescenza tecnica di un apparato, verificata e confermata in ogni caso dall'Ufficio ICT, è per convenzione di 3 anni per apparati quali cellulari e similari e 5 anni per Notebook o PC che non svolgano funzioni tecniche avanzate e/o di managing e monitoring della rete o di altri apparati. Questi ultimi strumenti, in cui sono inclusi anche cellulari e smartphone con funzioni avanzate (di cui sia accertato l'utilizzo) oltre a Notebook e PC, hanno tempi di obsolescenza di 1-2 anni per i primi e di 3 per i secondi. In ogni caso, per la sostituzione è necessaria la richiesta dell'Responsabile dell'Ufficio e la valutazione tecnica del Ufficio ICT che comunicherà, per iscritto, tale

richiesta al Direttore Operativo e/o Direttore Generale che autorizzeranno l'eventuale sostituzione. Sono esclusi da tali considerazione i server e gli apparati del CED che sono sostituiti o aggiornati in funzione delle necessità di calcolo o di storage richiesto dai servizi caricati su di essi e, comunque, su supervisione e monitoraggio del personale del CED.

Su richiesta dei Responsabili d'Ufficio sarà possibile riscattare gli apparati utilizzati al prezzo determinato dall'ammortamento contabile e/o dall'oggettivo prezzo di mercato del bene, solo quando ne sia sancita l'obsolescenza per l'utilizzo aziendale, cioè quando il Ufficio ICT non ritenga sia possibile o necessario il riutilizzo. Il Responsabile del Ufficio ICT produrrà un documento dove indicherà il prezzo e lo stato del bene, documento che sarà comunicato al Direttore Operativo e/o Direttore Generale che autorizzeranno il riscatto.

E', infine, possibile la Portability dei numeri aziendali nel caso in cui un dipendete termini il contratto di lavoro con l'azienda e voglia mantenere il numero assegnato. E' possibile anche la Portability contraria, cioè un nuovo dipendente a cui venga assegnata una SIM, voglia mantenere il suo numero privato.

Articolo XIV. Attuazione e variazioni

Il presente regolamento entra in vigore a decorrere dalla data 01/01/2015 e potrà essere modificato su richiesta dell'Ufficio ICT, previa autorizzazione del Responsabile dell'Ufficio referente del settore e validazione del Responsabile Qualità.

[1] Tutti i prodotti e le reti realizzate sono conformi ai standard nazionali ed internazionali. In particolare gli standard presi in maggiore considerazione, poiché internazionalmente riconosciuti ed attuati sono:

- EIA/TIA 568-B Commercial Building Telecommunications Cabling Standard 2001 e relative
- Addendum;
- EIAITIA 569-A Commercial Building Standard for Telecommunications Pathways and Spaces
- (ottobre 1990);
- EIA/TIA 570 Residential and Light Commercial Building Telecommunications Wiring Standard
- (Giugno 1991);
- EIA/TIA 607 Commercial Building Grounding and Bonding Requirements for Telecommunications

- (Agosto 1994);
- EIA/TIA 606-A Administration Standard for Commercial Telecommunications Infrastructure;
- ISO/IEC International Standard 11801 2 nd Edition (Settembre 2002);
- CENELEC EN 50173 2 nd Edition (ratificata in novembre 2002);
- CEI 306-6;
- EN 50173.

Inoltre, nella scelta dei materiali, sono state tenute in considerazione le seguenti raccomandazioni:

- tutti i materiali e gli apparecchi impiegati sono adatti all'ambiente in cui vengono installati e sono tali da resistere alle azioni meccaniche, corrosive, termiche o dovute all'umidità, alle quali potrebbero essere esposti durante l'esercizio;
- tutti i materiali impiegati hanno dimensioni e caratteristiche tali da rispondere alle norme CEI ed alle tabelle CEI-UNEL attualmente in vigore;
- in particolare, tutti gli apparecchi ed i materiali installati sono muniti del contrassegno IMQ (marchio italiano di qualità) che ne attesti la rispondenza alle normative vigenti oppure essere comunque muniti di Marchio di Qualità riconosciuto a livello internazionale.

Nella realizzazione delle reti sono stati tenuti in considerazione i requisiti definiti per la compatibilità elettromagnetica (EMC) di una linea di trasmissione che sono raggruppati in appositi standard facenti capo ad indicazioni FCC (Federal Communications Commission) o EN (European Norm). Sono, infatti, limitati sia l'energia radiante, che potrebbe interferire con altri dispositivi elettronici presenti nell'area, nonché gli effetti dell'energia incidente, che potrebbe generare rumore sul cavo.

Le reti sono realizzate con fibre monomodali o multimodali a seconda dei casi e con cavo di tipo UTP cat.5e o cat.6e, rispettando l'applicazione dei principali accorgimenti di installazione quali:

- i cavi sono installati in modo tale che non si creino piegature o curvature eccessive;
- i cavi sono installati senza giunti da un punto all'altro;
- i cavi sono utilizzati con il minimo di trazione;
- i cavi non sono posati direttamente all'interno di controsoffittature o pannelli senza appositi cavidotti, o legati a cavi di sospensione del sistema di illuminazione;
- i cavi sono identificati con etichette;

[2] D. LSG 196/2003