REGOLAMENTO DATA CENTER

VERSIONE	DATA	AUTORE	STATO
1.0	02/05/2013	Matteo Righetti	Finale

RIVISTO DA	DATA REVISIONE
Massimo Russo	02/05/2013
Stefano Montano	02/05/2013

APPROVATO DA	DATA APPROVAZIONE
Luciano Longhi	02/05/2013

STORIA DEL DOCUMENTO

VERSIONE	DATA	AUTORE	MODIFICHE
0.1	20/02/2013	Matteo Righetti	Prima stesura
0.2	07/03/2013	Matteo Righetti	Revisione di Massimo Russo, piccole integrazioni
0.3	19/04/2013	Matteo Righetti	Integrazioni per convenzione INFN
1.0	02/05/2013	Matteo Righetti	Versione approvata

INDICE

1. Informazioni generali

1.1. Scopo del documento

Il presente regolamento ha l'obiettivo di garantire il miglior utilizzo e mantenimento possibile per i Data Center del Centro InfoSapienza, in modo da assicurare costantemente gli adeguati livelli di funzionalità, sicurezza, accessibilità, affidabilità di tutte le risorse incluse, al fine di rendere disponibile un ottimale ambiente fisico per l'erogazione di servizi chiave per l'intera Università.

Il regolamento norma i diversi aspetti connessi con la gestione e l'utilizzo dei Data Center, relativi a:

- procedure e modalità di accesso,
- regole di gestione delle risorse (informatiche ed infrastrutturali),
- regole di comportamento da parte degli utenti.

1.2. Ambito di applicazione

Il regolamento si applica a tutte le risorse ed a tutto il personale interessato nell'accesso, nell'utilizzo e nella gestione dei Data Center di cui è dotato il Centro InfoSapienza, così come indicati nel capitolo 2.

In particolare sono soggetti destinatari del regolamento:

- il personale del Centro InfoSapienza deputato alla gestione ed alla manutenzione dei Data Center;
- il personale interno al Centro InfoSapienza fruitore dei servizi e delle risorse dei Data Center;
- il personale dell'Università o di terze parti fruitore dei servizi e delle risorse dei Data Center, soprattutto quando riveste anche un ruolo attivo di responsabilità di gestione e manutenzione di alcune risorse;
- il personale di terze parti incaricato di attività di gestione o manutenzione su quota parte dei servizi e delle risorse dei Data Center.

Tali soggetti hanno tutti la responsabilità di rispettare le regole e le procedure riportate nel documento, a pena di sanzioni (capitolo 6).

1.3. Normative applicabili

Ad integrazione delle disposizioni indicate nel presente regolamento, si rimanda alla normativa vigente applicabile relativamente alla sicurezza sul lavoro, ossia al Decreto Legislativo n. 81 del 9 aprile 2008, anche noto come "Testo unico in materia di salute e sicurezza sul lavoro", e alle relative disposizioni correttive, ovvero al Decreto legislativo 3 agosto 2009 n. 106 e a successivi ulteriori decreti. Per maggiori informazioni si rimanda al link http://www.lavoro.gov.it/lavoro/sicurezzalavoro/MS/Normativa/default.

Si ritiene utile anche ricordare la normativa in tema di smaltimento dei rifiuti (in particolare i Rifiuti da Apparecchiature Elettriche ed Elettroniche – RAEE) e rispetto ambientale:

- D.Lgs. 151/2005 e ss.mm.ii.,
- D.Lgs. 152/2006 e ss.mm.ii.,
- D.M. 65/2010,
- D.M. 17 dicembre 2009 – SISTRI – recante l'istituzione del nuovo sistema di controllo della tracciabilità dei rifiuti e ss.mm.ii..

Infine, per ogni evenienza non espressamente riportata nel presente regolamento, si applicano le norme previste dai Codici Civile e Penale, che nel caso specifico prevede:

- Art. 635 C.P.. *Danneggiamento*. Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui, è punito, a querela della persona offesa, con la reclusione fino a un anno o con la multa fino a euro 309. La pena è della reclusione da sei mesi a tre anni e si procede d'ufficio, se il fatto è commesso (...) su cose esistenti in uffici o stabilimenti pubblici (n.7 dell'art.625 C.P.).

- Art. 635-bis C.P.. *Danneggiamento di sistemi informatici e telematici*. Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

1.4. Eccezioni

In taluni casi e sotto la diretta responsabilità del personale responsabile della gestione dei Data Center (rif. §1.6), le disposizioni riportate nel presente regolamento possono essere oggetto di sospensione o deroga.

In particolare, ciò può avvenire:

- in situazioni critiche, per contrastare rischi e minacce sia alle risorse umane che fisiche che informatiche;
- in situazioni di opportunità e convenienza, qualora valutate come tali dal suddetto personale responsabile della gestione dei Data Center o per approvazione esplicita degli stessi in forma scritta (anche elettronica) su richiesta dei destinatari fruitori.

In ogni caso le eccezioni non possono derogare la normativa vigente (rif. §1.3) né i piani e le procedure di prevenzione e protezione dai rischi predisposte dall'Ateneo né i princìpi generali di sicurezza e tutela delle risorse e dei lavoratori.

1.5. Validità

Il presente regolamento è in vigore dalla data di ultima approvazione, da parte del Direttore del Centro InfoSapienza, ed ha validità a tempo indeterminato.

Il documento deve essere sottoposto ad un processo di revisione e aggiornamento (con approvazione finale) almeno annuale e comunque nei casi in cui nuove condizioni o finalità richiedano correzioni o integrazioni al suo contenuto.

Si stabilisce al 31 Gennaio di ogni anno il termine entro il quale deve essere concluso il processo di revisione e approvazione annuale. In ogni caso, trascorso tale termine, il regolamento si intende approvato automaticamente per altri 12 mesi.

1.6. Riferimenti

Di seguito si riportano i riferimenti delle principali figure menzionate e/o coinvolte nelle procedure indicate nel presente documento:

- **Responsabile Data Center**
  - Nome: Stefano Montano
  - E-mail: stefano.montano@uniroma1.it
  - Telefono fisso: +39 06 49690280 (ext) – 30280 (int)
  - Telefono mobile: +39 331 6994392
- **Capo Settore per i Sistemi Centrali e per l'Office Automation**
  - Nome: Massimo Russo
  - E-mail: massimo.russo@uniroma1.it
  - Telefono fisso: +39 06 49910158 (ext) – 20158 (int)
  - Telefono mobile: +39 348 2258481
- **Servizio di Assistenza e Supporto per i Data Center InfoSapienza**
  - E-mail: datacenter-infosapienza@uniroma1.it

- **Servizio di Vigilanza di Ateneo**
  - Società: Sipro
  - Telefono fisso: 8108 (numero di emergenza interno)
    Esterno: 06/49694231 – 06/49694233
    Interno: 34231 – 34233
    Cellulare: 348/0037520 – 349/3318774

1.7. Acronimi

DC	Data Center
RDC	Responsabile dei Data Center
SAS	Servizio di Assistenza e Supporto per i Data Center InfoSapienza
SSCOA	Settore per i Sistemi Centrali e per l'Office Automation

2. Data Center

Il Data Center (DC) è un locale attrezzato, normalmente non presidiato da personale tecnico, che ha la funzione di contenere sistemi di elaborazione con funzionalità server e storage, apparati di rete locale, apparati di rete geografica e apparati di telefonia, per l'erogazione di servizi informatici e telematici.

L'ambito di applicazione del seguente regolamento è costituito dai due DC in gestione da parte del Centro InfoSapienza:

- INFO1: situato nel piano seminterrato dell'Edificio di Giurisprudenza (codice U-GOV CU002), con ingresso dal lato Rettorato;
- INFO2: situato nel piano seminterrato dell'Edificio "Enrico Fermi" di Fisica (codice U-GOV CU033), presso i locali dell'ex-C.I.T.I.Co.R.D..

Nel DC sono installati strumenti e sistemi idonei a garantire l'adatta collocazione e il corretto funzionamento delle apparecchiature contenute:

- arredamento tecnico per il posizionamento degli apparati;
- armadi rack per l'installazione di apparati a moduli;
- impianti e connessioni per la fornitura elettrica, idrica e di connettività di rete;
- sistemi per l'interfaccia utente (unità KVM);
- sistemi di condizionamento dell'aria;
- sistemi di continuità elettrica;
- sistemi di rilevamento intrusioni;
- sistemi di rilevamento incendi, fumi e allagamenti;
- sistemi di spegnimento incendi.

Le attività consentite nel DC sono installazione e manutenzione degli apparati e sistemi, e controllo e manutenzione dei locali e delle dotazioni annesse. Tutte le attività, come richiesto e normato dal presente regolamento, devono essere realizzate con modalità che garantiscano costantemente la massima garanzia sullo stato di funzionamento, gestibilità e protezione delle risorse del DC e dei servizi erogati.

3. Gestione degli accessi

3.1. Livelli di accesso previsti

Sono previsti quattro livelli di accesso differenti, connessi al ruolo ed alle finalità associate alle varie tipologie di utenti ammessi (come indicati nel paragrafo 1.2):

- personale di servizio,
- accesso autonomo,
- accesso supervisionato,
- accesso ospiti.

Oltre al dover rispettare le regole generali (rif. §3.2), ogni livello presenta specifiche procedure di gestione degli accessi, illustrate nei paragrafi seguenti.

Gli utenti che non rientrano nelle casistiche previste e nel relativo livello di accesso associato, non possono accedere ai DC.

3.2. Regole generali

Ad eccezione dell'accesso accompagnatori, il permesso di accesso e l'assegnazione dello specifico livello di accesso sono strettamente personali e regolati sempre da un controllo ai varchi tramite tessera elettronica (badge), anch'essa assegnata sempre in maniera personale esclusiva.

Ne conseguono pertanto tutte le responsabilità personali dell'utente relativamente a:

- custodire costantemente il badge in maniera sicura, in modo da escluderne il possesso e l'uso, anche temporaneo, da parte di terzi, nonché la duplicazione;
- assicurarsi che ad ogni singolo accesso autorizzato tramite l'impiego di uno specifico badge, entri all'interno dei DC il solo utente assegnatario del bagde, salvo il caso di ospiti per il quale si rimanda alle norme specifiche (rif. §3.6);
- in caso di furto o smarrimento del badge, segnalare tempestivamente la perdita di possesso del badge al Servizio di Assistenza e Supporto (SAS) per i Data Center InfoSapienza;
- segnalare proattivamente il venir meno delle necessità o delle precondizioni per l'accesso ai DC, qualora ciò si verifichi prima della naturale scadenza del permesso di accesso accordato, in modo da anticipare responsabilmente la procedura di revoca/terminazione del permesso di accesso (rif. §3.3.3).

Il Centro InfoSapienza mantiene sui propri sistemi la registrazione di tutti gli accessi effettuati ai DC, associati univocamente al badge utilizzato per l'accesso: tali dati verranno utilizzati esclusivamente a posteriori, a fini di indagine in caso di incidenti alla sicurezza degli accessi, danneggiamenti, furti o altri eventi dolosi, o su richieste delle autorità giudiziarie.

Il Centro InfoSapienza si riserva il diritto di:

- revocare in qualsiasi momento, anche senza preavviso in casi eccezionali, il permesso di accesso ai DC, qualora si rilevino:
  - gravi rilievi comportamentali in capo all'utente,
  - elevati rischi di sicurezza connessi attivamente o passivamente all'attività dell'utente,
  - cause di forza maggiore;
- attivare verifiche periodiche sull'effettiva persistenza delle necessità o delle precondizioni per l'accesso ai DC, avviando anticipatamente, se opportuno, la procedura di terminazione del permesso di accesso (rif. §3.3.3);
- attivare verifiche periodiche sull'effettiva persistenza dei requisiti connessi alla concessione di un determinato livello di accesso, procedendo, se opportuno, all'assegnazione di un nuovo livello.

L'elenco completo degli utenti abilitati all'accesso ai DC verrà reso disponibile, su richiesta motivata, a tutti i referenti responsabili/titolari di risorse ospitate (e/o relativi servizi erogati) all'interno dei singoli DC, nonché ad organi interni o esterni all'Università titolati a tale richiesta (eventualmente a discrezione del Capo Settore per i Sistemi Centrali e per l'Office Automation – SSCOA – e previa autorizzazione da parte del Direttore del Centro InfoSapienza.

3.3. Personale di servizio

Tale categoria include esclusivamente personale in servizio presso il Centro InfoSapienza, che necessita di un accesso per la gestione e manutenzione diretta di risorse o servizi inerenti od ospitati all'interno dei DC.

3.3.1. Richiesta di accesso

Il personale in servizio presso il Centro InfoSapienza si intende automaticamente pre-autorizzato ad accedere ai DC.

Tuttavia, ai fini di garantire la piena gestibilità degli accessi da parte dei responsabili preposti, è richiesto l'invio di una comunicazione e-mail al SAS (rif. §1.6), indicando le seguenti informazioni:

- nome e cognome del dipendente da autorizzare;
- indirizzo e-mail del dipendente;
- matricola del dipendente;
- DC per cui si richiede l'accesso.

La richiesta può essere inviata dal responsabile di struttura a cui afferisce il dipendente oppure dal dipendente stesso avendo in copia conoscenza il responsabile di struttura.

E' comunque opportuno, al fine di mantenere una razionalizzazione degli accessi e la minore esposizione possibile ai rischi (di varia natura), che la richiesta sia originata da congrui motivi di necessità lavorativa, valutati congiuntamente dal responsabile di struttura e dal Capo SSCOA, e che tali motivi vengano rivalutati periodicamente e proattivamente.

Il personale di servizio è d'ufficio tenuto alla conoscenza ed accettazione del presente regolamento.

3.3.2. Modalità di accesso

Il personale di servizio autorizzato viene abilitato all'accesso ai DC tramite il medesimo badge personale già in possesso per la rilevazione dell'orario lavorativo.

Il personale di servizio può accedere autonomamente, senza preventiva comunicazione e senza supervisione.

3.3.3. Revoca/terminazione del permesso di accesso

Il permesso di accesso per il personale di servizio viene automaticamente revocato al 1 Marzo del secondo anno di validità dell'accesso (sia nel caso di primo rilascio che a seguito di rinnovo).

Il SAS provvede, almeno 15 giorni prima della data di scadenza della validità del permesso, a notificare all'utente ed al relativo responsabile di struttura l'approssimarsi dell'evento. E' responsabilità dell'utente e/o del responsabile di struttura inviare una richiesta di rinnovo del permesso di accesso, con modalità analoghe alla richiesta di primo rilascio (rif. §3.3.1).

Anche in caso di revoca o terminazione anticipata da parte del Centro InfoSapienza, nei casi previsti dalle regole generali (rif. §3.2), il SAS provvede ad inviare, con maggiore preavviso possibile, la notifica all'utente ed al relativo responsabile di struttura.

3.3.4. Richiesta di un nuovo badge

In caso di smarrimento, furto, deterioramento o malfunzionamento del badge di accesso, si rimanda alle relative procedure previste per il badge personale per la rilevazione dell'orario lavorativo, al fine di ottenere un nuovo badge.

3.4. Accesso autonomo

Tale livello di accesso viene di norma accordato al personale interno all'Università incaricato di operare su risorse ospitate (e/o relativi servizi erogati) all'interno dei DC, in maniera sufficientemente regolare (continuativa o con elevata frequenza), che presenti opportune credenziali e comprovate caratteristiche di affidabilità personale e professionale.

La concessione di tale livello di accesso è soggetta a valutazione da parte del Capo SSCOA ed eventualmente ad autorizzazione da parte del Direttore del Centro InfoSapienza.

3.4.1. Richiesta di accesso

La richiesta di accesso deve essere inviata via e-mail al SAS (rif. §1.6), indicando le seguenti informazioni:

- nome e cognome e struttura/società di appartenenza della persona da autorizzare;
- nome e cognome e struttura/società di appartenenza del responsabile organizzativo/funzionale della persona da autorizzare;
- indirizzo e-mail e numero di telefono (sia fisso che possibilmente mobile, per i casi di urgenza) della persona da autorizzare;
- matricola (se dipendente dell'Università) o estremi del documento di identità della persona da autorizzare;
- risorsa informatica di afferenza e DC ospitante;
- periodo di validità del permesso di accesso richiesto;
- motivazione della richiesta (in particolare ruolo/attività esercitate dalla persona da autorizzare).

La richiesta può essere inviata dal responsabile organizzativo/funzionale (possibilmente interno all'Università) a cui riporta la persona richiedente oppure dal richiedente stesso avendo in copia conoscenza il responsabile organizzativo/funzionale. L'invio deve avvenire con almeno 2 giorni di preavviso rispetto alla data di inizio del periodo di accesso richiesto.

La richiesta è soggetta a valutazione da parte del Capo SSCOA ed eventualmente ad autorizzazione da parte del Direttore del Centro InfoSapienza.

Qualora accettata, il SAS provvede a contattare ai recapiti indicati la persona segnalata. Nel caso generale il SAS prende accordi per il ritiro del badge di accesso, previa presentazione del documento di identità indicato nella richiesta; al momento del ritiro, il richiedente deve firmare una ricevuta di avvenuta consegna del badge e di accettazione del presente regolamento. Nel caso il richiedente sia un dipendente dell'Ateneo già in possesso del badge personale per la rilevazione dell'orario lavorativo (e che quindi non necessita di un nuovo badge specifico), il SAS fornisce indicazioni al richiedente per prendere visione del presente regolamento, che il richiedente è tenuto a visionare ed accettare anche senza dichiarazione esplicita.

Il SAS provvede quindi ad informare via e-mail il responsabile organizzativo/funzionale del richiedente circa l'avvenuta abilitazione e consegna del badge, comunicandone il relativo numero identificativo e la data di scadenza prevista.

3.4.2. Modalità di accesso

Gli utenti autorizzati vengono abilitati all'accesso ai DC tramite il badge personale consegnato in fase di richiesta di accesso o, se dipendenti dell'Università e laddove applicabile, tramite il medesimo badge personale già in possesso per la rilevazione dell'orario lavorativo. Gli utenti possono quindi accedere autonomamente, senza preventiva comunicazione e senza supervisione.

L'utente deve accedere ai DC indossando in maniera ben visibile il badge e avendo disponibile un proprio documento di identità; in qualsiasi momento durante la permanenza all'interno dei DC, il Responsabile dei Data Center (RDC) o un suo collaboratore possono richiedere all'utente di mostrare badge e documento di identità, al fine di verificare l'identità della persona ed il suo reale diritto di accesso.

3.4.3. Revoca/terminazione del permesso di accesso

Il permesso di accesso per gli utenti ad accesso autonomo viene revocato alla data di terminazione del periodo di accesso indicato nella richiesta (sia in caso di primo rilascio che di rinnovo).

Tuttavia, nel caso di accesso per lunghi periodi, il permesso viene automaticamente revocato il 1 Marzo del secondo anno di validità dell'accesso (sia in caso di primo rilascio che di rinnovo), salvo diversi accordi specifici.

Il SAS provvede, almeno 15 giorni (ove applicabile) prima della data di scadenza della validità del permesso, a notificare all'utente ed al relativo responsabile di struttura l'approssimarsi dell'evento. E' responsabilità dell'utente e/o del responsabile di struttura inviare in risposta un'eventuale richiesta di rinnovo del permesso di accesso, con modalità analoghe alla richiesta di primo rilascio (rif. §3.4.1).

Anche in caso di revoca o terminazione anticipata da parte del Centro InfoSapienza, nei casi previsti dalle regole generali (rif. §3.2), il SAS provvede ad inviare, con maggior preavviso possibile, la notifica all'utente ed al relativo responsabile di struttura.

A seguito della disattivazione, l'utente è tenuto alla riconsegna del badge (tranne il caso in cui l'utente abbia utilizzato per l'accesso il proprio badge personale per la rilevazione dell'orario lavorativo), entro 15 giorni dalla data di terminazione, da effettuarsi contattando il SAS e concordando le modalità di restituzione.

3.4.4. Richiesta di un nuovo badge

In caso di smarrimento, furto, deterioramento o malfunzionamento del badge di accesso, o in altre condizioni in cui si necessita comunque di un nuovo badge sostitutivo, se all'utente era stato consegnato un badge specifico di accesso ai DC, l'utente deve inviare una richiesta via e-mail al SAS (rif. §1.6), con modalità analoghe alla richiesta di primo rilascio (rif. §3.4.1). Anche la gestione della richiesta da parte del SAS segue la medesima procedura prevista per il primo rilascio.

In caso di deterioramento, malfunzionamento o altre condizioni in cui si richiede la sostituzione del badge, l'utente è tenuto obbligatoriamente a riconsegnare il badge in suo possesso, contestualmente al ritiro del nuovo badge.

Se invece l'utente utilizzava per l'accesso il medesimo badge personale per la rilevazione dell'orario di lavoro, si rimanda alle procedure previste per smarrimento, furto, deterioramento o malfunzionamento di tale tipologia di badge, al fine di ottenere un nuovo badge.

3.5. Accesso supervisionato

Tale livello di accesso viene di base accordato a personale che necessiti di accedere ed operare all'interno dei DC in circostanze occasionali (es. interventi di manutenzione straordinaria) o con bassa frequenza e/o che non presenti opportune credenziali e comprovate caratteristiche di affidabilità personale e professionale.

La concessione del permesso di accesso è soggetta a valutazione da parte del Capo SSCOA ed eventualmente ad autorizzazione da parte del Direttore del Centro InfoSapienza.

A giudizio del Capo SSCOA, la gestione dell'accesso supervisionato può essere delegato a utenti già autorizzati ad accedere come personale di servizio o con accesso autonomo, esclusivamente nell'ambito dell'accesso alle risorse di loro stretta competenza e per l'ingresso di non più di 2 persone contemporaneamente (indipendentemente dal numero di utenti autorizzati accompagnatori). In tal caso, gli utenti delegati assumono totalmente le responsabilità ed i doveri del ruolo di supervisore e sono tenuti a tenere comportamenti analoghi a quelli che terrebbero i responsabili della gestione dei DC.

In ogni caso non possono accedere in modalità supervisionata:

- minorenni;
- persone in condizioni psico-fisiche non idonee a permanere e spostarsi all'interno dei DC;
- persone che non presentino opportune credenziali e caratteristiche di affidabilità personale e professionale.

L'utente delegato che concede l'accesso è esclusivamente e inderogabilmente responsabile di:

- valutare il rispetto dei requisiti e delle condizioni richieste per le persone candidate all'accesso;
- istruire adeguatamente le persone supervisionate sulle caratteristiche dell'ambiente dei DC, sui rischi presenti, sulle norme comportamentali previsti dal presente regolamento e sulle procedure da attuarsi per prevenire o gestire situazioni di emergenza e di rischio per l'incolumità delle persone e la salvaguardia dei beni e del loro funzionamento;
- supervisionare costantemente la presenza delle persone all'interno dei DC, senza mai lasciarli soli o lontani dalla vista, e vigilare costantemente sul loro comportamento e sul rispetto delle norme comportamentali;
- fornire alle persone ospiti le prime e immediate direttive in caso si attivino, durante la permanenza all'interno dei DC, le procedure di gestione delle emergenze (di qualsiasi tipo), in attesa dell'intervento diretto del RDC o di altri addetti preposti dall'Ateneo a tali scopi.

3.5.1. Richiesta di accesso

La procedura seguente si applica nel caso standard di accesso supervisionato tramite il SAS. Ad eventuali altri utenti delegati alla gestione dell'accesso supervisionato viene raccomandato di seguire una procedura analoga.

La richiesta di accesso deve essere inviata via e-mail al SAS (rif. §1.6), indicando le seguenti informazioni:

- nome e cognome e struttura/società di appartenenza della persona da autorizzare;
- nome e cognome e struttura/società di appartenenza del responsabile organizzativo/funzionale della persona da autorizzare;
- indirizzo e-mail e numero di telefono (sia fisso che possibilmente mobile, per i casi di urgenza) della persona da autorizzare;
- estremi del documento di identità della persona da autorizzare;
- risorsa informatica di afferenza e DC ospitante;
- periodo di validità del permesso di accesso richiesto;
- motivazione della richiesta (in particolare ruolo/attività esercitate dalla persona da autorizzare).

La richiesta può essere inviata dal responsabile organizzativo/funzionale (possibilmente interno all'Università) a cui riporta la persona richiedente oppure dal richiedente stesso avendo in copia conoscenza il responsabile organizzativo/funzionale. L'invio deve avvenire con almeno 2 giorni di preavviso rispetto alla data di inizio del periodo di accesso richiesto, salvo situazioni di emergenza opportunamente motivate rispetto alle quali il Centro InfoSapienza fornirà la massima disponibilità possibile.

La richiesta è soggetta a valutazione da parte del Capo SSCOA ed eventualmente ad autorizzazione da parte del Direttore del Centro InfoSapienza.

Qualora accettata, il SAS provvede a contattare ai recapiti indicati la persona segnalata e concorda l'effettivo periodo di accesso ai DC, prendendo in considerazione eventuali vincoli ed esigenze operative del richiedente. Contestualmente, il SAS fornisce indicazioni al richiedente per prendere visione del presente regolamento, che il richiedente è tenuto a visionare ed accettare anche senza dichiarazione esplicita.

3.5.2. Modalità di accesso

Gli utenti autorizzati vengono abilitati all'accesso ai DC esclusivamente attraverso l'accompagnamento e la costante supervisione, per tutto il tempo di permanenza all'interno dei DC, di un referente del SAS (o utente autorizzato delegato, se del caso), nel periodo concordato in fase di richiesta del permesso di accesso.

All'utente, in fase di identificazione iniziale, può essere richiesto dal RDC o suoi collaboratori di mostrare un proprio documento di identità. Nel caso di delega, si raccomanda agli utenti autorizzati delegati di seguire un'analoga procedura.

3.6. Accesso ospiti

L'accesso ospiti rappresenta la possibilità, per un utente già autorizzato ad accedere come personale di servizio o con accesso autonomo, di introdurre in via eccezionale e per breve tempo nei DC persone terze accompagnatrici, purché l'accesso sia motivato da ragioni strettamente professionali e collegate all'attività propria dell'Università.

In ogni caso non possono accedere in qualità di accompagnatori ospiti:

- minorenni;
- persone in condizioni psico-fisiche non idonee a permanere e spostarsi all'interno del DC;
- persone che non presentino opportune credenziali e caratteristiche di affidabilità personale e professionale.

Le persone ospiti possono accedere ai DC esclusivamente a scopo illustrativo/didascalico, non potendo in nessun modo operare alcuna attività all'interno dei DC.

L'utente che concede l'accesso è esclusivamente e inderogabilmente responsabile di:

- valutare il rispetto dei requisiti e delle condizioni richieste per le persone candidate all'accesso ospiti;
- istruire adeguatamente le persone ospiti sulle caratteristiche dell'ambiente dei DC, sui rischi presenti, sulle norme comportamentali previsti dal presente regolamento e sulle procedure da attuarsi per prevenire o gestire situazioni di emergenza e di rischio per l'incolumità delle persone e la salvaguardia dei beni e del loro funzionamento;
- supervisionare costantemente la presenza delle persone ospiti all'interno dei DC, senza mai lasciarli soli o lontani dalla vista, e vigilare costantemente sul loro comportamento e sul rispetto delle norme comportamentali;
- fornire alle persone ospiti le prime e immediate direttive in caso si attivino, durante la permanenza all'interno dei DC, le procedure di gestione delle emergenze (di qualsiasi tipo), in attesa dell'intervento diretto del RDC o di altri addetti preposti dall'Ateneo a tali scopi.

3.6.1. Richiesta di accesso

L'accesso ospiti può avvenire, sotto la responsabilità dell'utente autorizzato ospitante e senza preventiva comunicazione al SAS, solo per un numero di ospiti accedenti contemporaneamente non superiore a 2 persone (indipendentemente dal numero di utenti ospi

tanti accompagnatori).

Per l'accesso di un maggior numero di persone ospiti, è obbligatorio l'invio via e-mail di una richiesta di accesso al SAS (rif. §1.6), indicando le seguenti informazioni:

- struttura/società di appartenenza delle persone ospiti;
- numerosità delle persone ospiti;
- nome e cognome e struttura/società di appartenenza dell'utente autorizzato ospitante;
- motivazione e finalità della visita.

La richiesta deve essere inviata dall'utente autorizzato ospitante e deve avvenire con almeno 2 giorni di preavviso rispetto alla data di accesso richiesto.

La richiesta è soggetta a valutazione da parte del Capo SSCOA ed eventualmente ad autorizzazione da parte del Direttore del Centro InfoSapienza.

3.6.2. Modalità di accesso

Gli utenti ospiti vengono abilitati all'accesso ai DC esclusivamente attraverso l'accompagnamento e la costante supervisione, per tutto il tempo di permanenza all'interno dei DC, dell'utente autorizzato ospitante.

All'utente ospite, in fase di identificazione iniziale, può essere richiesto dall'utente ospitante o dal RDC o suoi collaboratori, di mostrare un proprio documento di identità.

Si raccomanda all'utente ospitante di far sì che ogni utente ospite, all'inizio ed alla fine dell'accesso, firmi una registrazione del proprio accesso su apposito documento/registro conservato dall'utente ospitante stesso.

4. Regole di gestione e comportamento

4.1. Condizioni ambientali e fornitura dei servizi

4.1.1. Accessibilità e sicurezza degli ambienti

- L'accesso ai DC è consentito solamente usando i varchi protetti da serratura elettronica ed il badge di accesso in dotazione agli utenti autorizzati.
- L'uso delle uscite di sicurezza è consentito solo in caso di emergenza e provocherà l'attivazione dell'apposito allarme.
- Per motivi di sicurezza e per conservare la temperatura costante di esercizio, tutti i varchi di accesso devono restare aperti solamente per il tempo strettamente necessario al passaggio di persone e materiali.
- L'esecuzione di lavori di qualunque tipo deve essere concordata e approvata dal Capo SSCOA, al quale va preliminarmente presentato un piano descrittivo delle attività da svolgere e i tempi previsti di realizzazione.
- In particolare, specifica attenzione deve essere posta verso tutte quelle operazioni che prevedono il sollevamento del pavimento sopraelevato all'interno del quale passa il flusso di aria fredda necessario alla refrigerazione dei sistemi. La rimozione contemporanea di più di due mattonelle provoca uno squilibrio nelle pressioni e nelle temperature dei flussi di aria, causando uno squilibrio termico pericoloso. Si fa quindi divieto di rimuovere più di 2 unità di pavimento contigue e non oltre le 6 unità in totale.
- In ogni caso nessuna mattonella può essere rimossa senza il permesso del RDC e la supervisione sua o di un suo collaboratore.
- In caso di rimozione di mattonelle dal pavimento, lo spazio aperto deve essere segnalato agli utenti e cordonato con appositi dispositivi; lo spazio deve rimanere aperto per il tempo minimo necessario all'esecuzione delle attività richieste.
- In linea generale, ogni attività che prevede l'installazione di impianti o apparecchiature da porre sotto la pavimentazione sopraelevata deve essere sottoposta a specifica approvazione del Capo SSCOA; lo stesso criterio si applica a tutte quelle attività che prevedono la creazione di griglie e altre forature del pavimento.
- Forature o sezionamenti di mattonelle devono essere realizzate fuori dai locali del DC; se ciò non è possibile, è necessario adottare i più efficaci accorgimenti volti alla riduzione, al contenimento ed alla raccolta della polvere e del materiale residuo generati.
- Le porte degli armadi rack che ospitano server ed altri apparati informatici devono restare aperte per il tempo strettamente necessario alle operazioni di installazione e manutenzione degli apparati.

- I cablaggi di collegamento dati devono usare, dove presente, la canalizzazione aerea apposita. I cavi vanno stesi e fissati con sistemi rimovibili come fascette plastiche o fermasacco metallici.
- Ogni cavo deve essere etichettato su entrambi i capi, in maniera perfettamente leggibile, usando ove possibile etichette plastiche (Dymo) e che riportino chiaramente la destinazione e l'arrivo di ogni cavo. In particolare, per l'etichettatura dei cavi di collegamento elettrico, si rimanda al paragrafo 4.2.3.
- Il cablaggio all'interno di ogni armadio rack deve essere condotto ordinatamente ed in modo che non sia mai impedita la chiusura delle porte anteriori e posteriori e che sia accuratamente evitata l'ostruzione del flusso di aria di refrigerazione che attraversa gli apparati, sia frontalmente che posteriormente.

4.1.2. Condizionamento e qualità dell'aria

- Il livello di umidità dell'aria all'interno dei DC deve rimanere il più possibile all'interno dei valori 40% - 60%.
- Il livello di temperatura dell'aria all'interno dei DC deve rimanere il più possibile vicino ai 21 C° e comunque sempre all'interno dei valori 18 C° - 24 C°.
- Ogni attività all'interno dei DC deve essere tesa alla conservazione delle temperature e dei livelli di umidità ottimali, con particolare riferimento all'ispezionabilità ed all'accesso alle unità di condizionamento, le quali non devono mai essere ostruite, sia nelle parti esposte che nella parte impiantistica installata nel pavimento sopraelevato.
- Ogni alterazione alle apparecchiature di condizionamento deve essere preventivamente concordata con il Capo SSCOA, approvata e documentata con nota scritta.
- Eventuali aperture verso l'esterno destinate al solo ricambio d'aria (es. finestre; si escludono pertanto i varchi di accesso – si veda il paragrafo 4.1.1), possono essere aperte esclusivamente in caso di criticità, per aumentare il flusso d'aria e/o contenere l'innalzamento di temperatura a fronte di malfunzionamenti dell'impianto di condizionamento a freddo dell'aria. All'operazione è abilitato esclusivamente il RDC o suoi collaboratori, previa autorizzazione da parte del Capo SSCOA. L'apertura va mantenuta per il minimo tempo necessario alla risoluzione della situazione critica.

4.1.3. Fornitura di energia elettrica

- I cablaggi relativi all'alimentazione elettrica devono passare negli appositi percorsi interni alla pavimentazione sopraelevata, usando materiali rispondenti alle normative CEI EN 60529 IP 54 (protezione da infiltrazione di polvere e resistenza agli spruzzi d'acqua).
- Il collegamento elettrico di ogni armadio rack presente all'interno dei DC deve essere eseguita da personale addestrato e solo dietro esplicita e documentata autorizzazione del Capo SSCOA, previa formalizzazione dei requisiti tecnici del collegamento e della disponibilità di energia elettrica richiesta.
- I cavi di alimentazione devono essere compatibili con le unità di distribuzione elettrica (PDU) presenti in ogni armadio rack, dotati di cavo di terra e certificati per carichi di almeno 16A.
- Ogni unità installata deve venir alimentata con doppia alimentazione proveniente da due quadri di distribuzione separati. Non sono ammesse unità prive di doppio alimentatore, salvo esplicita autorizzazione da parte del Capo SSCOA con nota scritta.
- I cavi di alimentazione devono essere etichettati A e B in relazione alla PDU di allaccio.
- Ogni collegamento elettrico all'interno dei DC è installato per scopi specifici; pertanto, nessun collegamento può essere usato senza l'approvazione del RDC o del Capo SSCOA.
- Solo personale tecnico addestrato autorizzato dal Capo SSCOA può aprire o modificare i pannelli elettrici o le PDU presenti all'interno dei DC.
- Solo personale tecnico addestrato autorizzato dal Capo SSCOA può realizzare modifiche all'impianto di fornitura di energia elettrica del DC.
- L'uso di strumenti elettrici (es. macchinari per pulizia) all'interno dei DC deve essere autorizzato dal Capo SSCOA e deve impiegare prese elettriche apposite; è fatto assoluto divieto di utilizzare a tale

scopo le PDU presenti negli armadi rack. Se richieste, prolunghe e prese multiple vengono fornite dal RDC o un suo collaboratore.

4.1.4. Pulizia degli ambienti

- E' fatto divieto di introdurre cibi e bevande all'interno dei DC.
- I locali dei DC devono riceve una pulizia straordinaria annuale sia sopra che sotto il pavimento sopraelevato (dove presente), inclusiva di: pulizia attorno ai cablaggi sotto la pavimentazione, pulizia energica dei pavimenti, rimozione della polvere dagli armadi rack, in particolare sulle superfici superiori e nelle aree aperte intorno agli armadi. Le attività di pulizia straordinaria devono essere eseguite da personale tecnico addestrato autorizzato dal Capo SSCOA, sotto la supervisione del RDC.
- Il RDC deve assicurarsi che il personale dedicato alla pulizia ordinaria settimanale sia adeguatamente formato sui rischi, i vincoli e le modalità di comportamento del personale all'interno dei DC e dei locali di servizio connessi.
- Ogni referente responsabile/titolare di risorse ospitate all'interno dei DC è tenuto a garantire la pulizia delle superfici delle proprie risorse, almeno 2 volte l'anno. Il RDC può segnalare al referente l'eventuale necessità di procedere ad una pulizia più frequente di 2 volte l'anno.
- Nessun liquido o fluido utilizzato per le attività di pulizia deve essere lasciato incustodito all'interno dei DC. Non è permesso l'utilizzo di prodotti ad alta concentrazione di ammoniaca o cloro né altro materiale che possa considerarsi corrosivo o infiammabile.

4.2. Infrastruttura IT

4.2.1. Modifiche e cambiamenti

- Tutte le modifiche e i cambiamenti all'interno dei DC, inclusi ma non limitati alle modifiche all'infrastruttura, aggiunta o rimozione di risorse, manutenzioni ordinarie pianificate o straordinarie di urgenza, prove di affidabilità e disponibilità dei sistemi di riserva, devono essere approvate dal Capo SSCOA e coordinate dal RDC.
- Nessun materiale (es. hardware, arredi, scaffalature, ecc.) può essere rimosso o aggiunto all'interno del Data Center senza preventiva richiesta ed approvazione da parte del Capo SSCOA o del RDC
- Tutte le modifiche alla dislocazione, le rimozioni e le aggiunte di risorse all'interno dei DC devono essere coordinate con il RDC per garantire il corretto aggiornamento della documentazione relativa al layout dei DC.

4.2.2. Installazione di nuove componenti

- Ogni occupazione significativa di spazio all'interno dei DC, anche se provvisoria e di breve durata, deve essere comunicata al RDC ed eventualmente approvata dal RDC o dal Capo SSCOA.
- Tutte le risorse informatiche devono essere montabili all'interno di armadi rack, secondo le indicazioni del Capo SSCOA. Eventuali eccezioni devono essere approvate dal Capo SSCOA con nota scritta.
- In base al livello di accesso assegnato e/o ad autorizzazioni specifiche concesse, è possibile che l'installazione di risorse all'interno dei DC sia effettuato direttamente dai referenti responsabili/titolari delle risorse e/o da collaboratori o terze parti autorizzate all'accesso, purché in possesso dei requisiti tecnici e normativi. Durante e dopo le attività di installazione, il Capo SSCOA e il RDC possono procedere a verifiche ispettive volte ad accertare il rispetto delle prescrizioni previste dal presente regolamento e/o altri regolamenti generali applicabili a livello di Ateneo e normative nazionali. In caso si rilevino non conformità, il referente responsabile/titolare delle risorse è tenuto a garantire la riparazione/rifacimento/sostituzione nel minor tempo possibile.

4.2.3. Documentazione ed etichettatura

- La cablatura di rete deve utilizzare la seguente colorazione standard:
  - colore grigio chiaro per bretelle ethernet di connessione tra gli "switch top of the rack";
  - colore blu per le connessioni all'interno degli armadi rack di rete, tra i patch panel e gli apparati attivi.
- Ogni referente responsabile/titolare di risorse all'interno dei DC deve rendere disponibile un'adeguata documentazione per la risoluzione tempestiva di eventuali problemi e criticità. La documentazione deve essere fornita al Capo SSCOA ed al RDC; quest'ultimo provvede alla sua archiviazione ordinata e conservazione.
- Tutti i server e le altre risorse devono essere etichettate con informazioni identificative. Tali informazioni devono essere leggibili e seguire un formato uniforme all'interno di tutti i DC. Le informazioni minime necessarie devono riportare: nome e cognome del referente del server, nome del server, nome del servizio erogato, numero della porta KVM di amministrazione, indirizzo IP primario di gestione e, opzionalmente, un telefono cellulare del referente.
- Tutti i collegamenti elettrici devono presentare affisse delle etichette (ad entrambi le terminazioni) che identificano il circuito e l'unità di distribuzione a cui sono attaccati, nonché riportino eventuali usi specifici, l'amperaggio, il voltaggio, il tipo di cavo, il tipo di connettore e la posizione nel quadro di entrambe le terminazioni (laddove applicabile) e la lunghezza del cavo. E' opportuno che le informazioni siano comprensibili e significative per qualsiasi persona ne abbia necessità e/o interagisca con il collegamento.
- Le informazioni presenti nelle etichettature e nella documentazione devono essere mantenute costantemente aggiornate a fronte di cambiamenti all'interno dei DC.

4.2.4. Rimozione di componenti

- Tutte le risorse dismesse devono essere rimosse quanto prima dai DC. Eventuali giacenze a tempo determinato o indeterminato devono essere approvate dal Capo SSCOA e annotate nella documentazione dei DC.
- Tutti i cavi attestati su apparati attivi o passivi non più utilizzati dovranno essere disconnessi dagli stessi e, ove possibile, rimossi immediatamente dalle canaline aeree.

4.3. Norme di comportamento per gli utenti

4.3.1. Comportamento in sala

- Ogni utente deve comportarsi in maniera giudiziosa, responsabile e professionale in ogni momento di permanenza all'interno dei DC, nell'assoluto rispetto del personale di servizio, degli altri utenti, della struttura, dell'ambiente e dei beni presenti nei DC.
- E' fatto divieto di introdurre cibi e bevande all'interno dei DC.
- E' fatto divieto di introdurre armi, esplosivi, materiali pericolosi, alcool, droghe e altri intossicanti, strumenti elettromagnetici che possono interferire con le risorse informatiche, materiali radioattivi.
- I DC devono essere manutenuti il più possibile puliti. Ogni persona che accede ai DC è tenuta a mantenere pulito il proprio spazio di azione.
- Gli strumenti utilizzati non devono mai essere lasciati incustoditi ed al termine dell'utilizzo devono sempre venire riposti nella sede assegnata.
- Gli utenti autorizzati non devono assolutamente interagire o intervenire su risorse non di loro pertinenza.
- Sono vietate riprese e fotografie all'interno dei DC, salvo espressa autorizzazione del Capo SSCOA e supervisione del RDC.
- E' ammesso l'uso di telefoni cellulari per traffico voce e dati.

- E' obbligatorio informarsi ed aderire ai Piani ed alle procedure di Prevenzione e Protezione dai Rischi vigenti all'interno dell'Ateneo e dei DC, finalizzate al mantenimento della sicurezza e della incolumità di persone e beni.
- E' fatto divieto assoluto di fumare.
- E' proibito l'immagazzinamento all'interno dei DC di materiale cartaceo e altro materiale combustibile/ infiammabile di qualsiasi tipo.
- E' proibito bloccare o ostruire in qualsiasi momento i varchi di accesso, le uscite di sicurezza, le sonde di rilevazione dei sistemi di allarme, il sistema di spegnimento incendi.
- Al momento dell'accesso e dell'uscita, ogni utente deve accertarsi dell'effettiva richiusura del varco di accesso, per prevenire l'intrusione di persone non autorizzate.

4.3.2. Gestione dei materiali

- Ogni risorsa in ingresso o in uscita dai DC deve essere imballata o disimballata all'esterno dei DC. Eventuali eccezioni devono essere approvate dal Capo SCCOA.
- Ogni materiale di scarto, materiale di imballaggio o di protezione e ogni rifiuto, introdotto o prodotto all'interno dei DC, deve essere rimosso appena possibile e comunque entro la giornata lavorativa.
- Ogni materiale lasciato inutilizzato sul pavimento o in punti non idonei dei DC, deve venir rimosso dal RDC o sui collaboratori e spostato in apposite aree di deposito.
- Quando possibile o richiesto, il SAS e/o il RDC coordina la consegna o la spedizione di risorse interne ai DC. Rimane comunque responsabilità del referente responsabile/titolare della risorsa procedere all'accettazione ed alle verifiche di qualità del caso.

4.3.3. Segnalazioni di non conformità o infrazioni

- Ogni situazione di non conformità o infrazione al presente regolamento o alle normative nazionali vigenti deve venire segnalata al RDC e/o al Capo SSCOA.
- Ogni utente dei DC è tenuto a segnalare proattivamente e tempestivamente i casi di cui ha evidenza o ragionevole sospetto, soprattutto riguardo a non conformità/infrazioni che mettano a rischio la sicurezza e incolumità di persone e beni.
- Il RDC e/o il Capo SSCOA devono attivare immediatamente tutte le azioni necessarie per il contenimento dei rischi e degli effetti della non conformità/infrazione fino alla risoluzione della stessa. Se necessario, a tale scopo possono coinvolgere e far intervenire organi di livello superiore all'interno dell'Ateneo.
- Nei casi più rilevanti, il RDC e/o il Capo SSCOA provvedono a segnalare, ove opportuno, coinvolgendo il Direttore del Centro InfoSapienza, i soggetti responsabili della non conformità/infrazione a organi terzi interni e/o esterni all'Ateneo preposti al controllo ed al sanzionamento (rif. §6) dei comportamenti lesivi.

4.3.4. Situazioni di emergenza

- Ogni situazione di emergenza deve venire segnalata, nelle ore diurne, al primo riferimento utile fra quelli indicati nel presente regolamento (rif. §1.6), mentre nelle ore serali e notturne (dalle ore 20:00 alle ore 8:00) deve obbligatoriamente essere segnalata al Servizio di Vigilanza dell'Ateneo.
- Ogni utente dei DC è tenuto a segnalare proattivamente e tempestivamente le situazioni di emergenza in divenire o in atto, soprattutto riguardo alle minacce più critiche (es. incendi, allagamenti, ecc.).
- Gli utenti sono tenuti a seguire scrupolosamente i piani e le procedure generali di gestione delle emergenze predisposte dall'Ateneo o eventuali indicazioni in specie impartite direttamente dai responsabili della gestione dei DC.

- In caso di emergenze relative alle risorse informatiche, il Centro InfoSapienza può procedere all'attivazione dei Piani di Continuità Operativa e Disaster Recovery, alla cui documentazione si rimanda per le specificità del caso.

5. Condizioni speciali

L'Università e/o il Centro InfoSapienza possono attivare specifici accordi di fornitura/condivisione dei servizi e delle risorse dei Data Center verso entità e utenze dell'Università o di terze parti, per le quali si applicano condizioni particolari che possono in parte derogare alle regole generali di gestione e comportamento.

Nei paragrafi seguenti vengono specificati gli accordi e le condizioni vigenti alla data di ultima approvazione delle presente regolamento.

Per quanto non espressamente indicato, si applicano in toto le regole generali di gestione e comportamento illustrate nei precedenti capitoli.

5.1. Convenzione INFN

Sulla base della Convenzione Quadro di durata quinquennale stipulata in Roma il 15 Maggio 2012 tra l'Università degli Studi di Roma "La Sapienza" e l'Istituto Nazionale di Fisica Nucleare (INFN) e la successiva Convenzione Operativa stipulata in Roma il 18 Febbraio 2013, viene concessa ad uso esclusivo all'INFN, in collaborazione con il Dipartimento di Fisica dell'Università, parte dell'area del Data Center INFO2 (rif. §2).

In particolare:

- Viene concesso un livello di accesso autonomo a tutto il personale dell'INFN e del Dipartimento di Fisica interessato alle risorse ospitate all'interno dell'area dedicata del Data Center INFO2, sulla base delle richieste avanzate dai responsabili organizzativi/funzionali dei due enti secondo la procedura standard (rif. §3.4); ogni richiesta è da intendersi pertanto implicitamente pre-autorizzata dal Capo SSCOA e dal Direttore del Centro InfoSapienza.
- Viene altresì concessa la delega per l'accesso supervisionato e l'accesso ospiti, nel rispetto dei criteri e delle condizioni indicati nei capitoli 3.5 e 3.6 rispettivamente, ma senza limiti di numerosità in termini di persone accedenti contemporaneamente; viene tuttavia richiesto che, in caso di accesso di più di 4 persone contemporaneamente, venga inviata una segnalazione via e-mail al SAS (rif. §1.6) con almeno 1 giorno di preavviso rispetto alla data di inizio dell'accesso e con l'indicazione della numerosità delle persone accedenti e del periodo di accesso previsto.
- Viene garantita massima autonomia ai due enti per quanto riguarda attività e lavori da eseguire nella propria area dedicata all'interno del Data Center e per la progettazione ed evoluzione della propria infrastruttura IT, purché le attività, i lavori e le modifiche:
  - non riguardino componenti infrastrutturali comuni di qualsiasi tipo, quali a titolo di esempio non esaustivo le mura, il pavimento reale e quello sopraelevato, la controsoffittatura, l'impiantistica, la fornitura di energia elettrica, ecc., quand'anche posizionate all'interno dell'area dedicata;
  - non impattino negativamente né mettano a repentaglio la sicurezza (anche di persone e beni), le prestazioni e la gestibilità dell'ambiente complessivo, delle componenti infrastrutturali comuni, delle risorse non di propria pertinenza;
  - non prevedano rischi convenzionali o specifici diversi rispetto a quelli che il Centro InfoSapienza ha già valutato come inerenti alle caratteristiche ed alle funzioni del Data Center, derivanti dalla presenza e/o funzionamento di:
    - rete fognaria,
    - impianto di distribuzione di acqua,
    - impianto di distribuzione di energia elettrica,
    - impianto di ventilazione ed areazione,
    - impianto di condizionamento dell'aria,

- rete telefonica e di trasmissione dati,
- impianto antincendio a schiuma/polvere/gas,
- rumore,
- pavimentazione sopraelevata con aperture.

Nell'ambito di tali esclusioni, si applicano in toto i criteri e le condizioni indicate nei capitoli 4.1 e 4.2.

Viene comunque richiesto che gli interventi di significativa entità vengano preventivamente segnalati per conoscenza al Capo SSCOA.

Rimane responsabilità dell'INFN e/o del Dipartimento di Fisica procedere alla valutazione dei rischi da interferenza ed alla redazione del relativo Documento Unico di Valutazione dei Rischi da Interferenza (DUVRI), nei casi e nelle modalità previste per legge, eventualmente acquisendo le necessarie informazioni dal Centro InfoSapienza per quanto di relativa competenza.

6. Sanzioni

Il mancato rispetto o la violazione delle norme previste dal presente regolamento sono passibili in primis di sanzioni limitative nell'accesso ai DC ed ai servizi fruiti, attraverso la revoca parziale o totale dei permessi di accesso e l'eventuale rimozione delle risorse informatiche dai DC.

Nei casi più rilevanti, il Centro InfoSapienza provvederà a segnalare i responsabili identificati a organi terzi interni e/o esterni all'Ateneo preposti al controllo ed al sanzionamento dei comportamenti lesivi.

Danni a persone o beni e infrazioni alle normative nazionali verranno perseguiti secondo la Legge.