

ALLEGATO 1

RETE DI ATENEO: descrizione, servizi e disposizioni operative di utilizzo

INDICE

- *Rete dati*
 - *Descrizione fisica e logica.*
 - *Protocolli ed indirizzamento*
 - *Principali Servizi:*
 - *Sicurezza*
 - *DNS*
 - *Autenticazione di Ateneo*
 - *Posta elettronica d'Ateneo*
 - *Accesso rete wireless*
 - *Accesso banche dati on-line*
 - *Accesso rete aule didattiche*
 - *Accesso remoto*
 - *Servizi agli studenti*
- *Rete Fonia*
 - *Descrizione sistema fonia*
- *Disposizioni operative dei siti web d'Ateneo*
 - *Modulo di richiesta nomi siti web*
- *Disposizioni operative per l'accesso alla rete dalle aree attrezzate per servizi rivolti agli studenti o al pubblico (laboratori informatici)*
- *Disposizioni operative per gli applicativi gestionali in rete*
- *Disposizioni operative per l'accesso alla rete dalla residenza universitaria Edificio U12*
 - *modulo di autorizzazione al trattamento dei dati personali*

RETE DATI

Descrizione fisica e logica

Per Rete di Ateneo si intende l'infrastruttura che permette lo scambio di dati e l'accesso ai servizi di rete internamente ed esternamente all'Ateneo.

La parte passiva di questa infrastruttura è costituita dal cablaggio in rame e in fibra ottica realizzato secondo gli standard internazionali del cablaggio strutturato.

La parte attiva è l'insieme degli apparati di rete (multilayer switch, router, firewall, access gateway ed access point) che ne costituiscono l'architettura e la logica di funzionamento anch'essa basata sulle più recenti specifiche standard internazionali di alta disponibilità, fault tolerance e scalabilità per reti multiservizio IP/MPLS.

Ogni edificio universitario ospita un locale tecnico, detto centro stella, collegato agli altri centri stella di edificio tramite collegamenti ridondati in fibra ottica, ponti radio e collegamenti geografici (questi ultimi forniti da network provider) che realizzano la dorsale di campus secondo il modello parzialmente magliato ed illustrata in figura 1.

Nel centro stella dell'edificio universitario U7, detto centro stella di Ateneo, sono ospitati i collegamenti geografici che permettono l'interconnessione della Rete di Ateneo con la rete nazionale della ricerca (Rete GARR) e, quindi, con l'Internet mondiale.

In ogni centro stella d'edificio sono concentrate anche le dorsali in fibra ottica che collegano, secondo il modello a stella, ai vari locali tecnici presenti sui diversi piani. Da ogni locale tecnico di piano, detto locale tecnico di distribuzione, si diramano cavi in rame e fibra ottica che realizzano i collegamenti con le postazioni utente (Fig. 2).

La parte attiva della rete prevede l'utilizzo di layer2 switch nei locali tecnici di distribuzione e di multilayer switch ad architettura non bloccante (core router veloci) nei centri stella di ogni edificio. L'architettura di rete implementata ha prestazioni di livello "carrier class" e ridondanza in ogni componente attiva onde garantire la mancanza di "single points of failure". La famiglia di standard utilizzata per la trasmissione su rete cablata è IEEE 802.3 con velocità 10/100/1000 Mbps per il livello di accesso, 2 Gbps per il livello di distribuzione e 10 Gbps per il livello di core. Le zone con copertura wireless si basano sui protocolli 802.11. Il backbone implementa MPLS ed i protocolli supportati sono quelli della suite IP con gli standard IETF ad essa correlati.

Con *presa Utente interna* si definisce il punto di connessione fonia/dati (nodo terminale), al quale può essere collegato un unico Sistema in Rete (computer, terminale, stampante, periferica o dispositivo, telefono, fax). Gli apparati di rete, a qualunque livello del modello di riferimento ISO/OSI lavorino (ad esempio hub, switch, router, access point), non sono considerati Sistemi in Rete. Ogni eccezione, anche temporanea, dovrà essere preventivamente concordata ed autorizzata dall'Amministratore di Sistema di Ateneo.

L'Amministratore di Sistema di Ateneo assicura in modo esclusivo e tempestivo la gestione, il monitoraggio, l'aggiornamento ed ampliamento della rete dell'Ateneo (cablaggio e parte attiva) sia sotto l'aspetto fisico che logico, curandone i relativi progetti, fino alla presa Utente compresa.

Il monitoraggio e la responsabilità amministrativa e tecnica per i Sistemi in Rete a valle della presa Utente sono di competenza del Referente informatico di struttura.

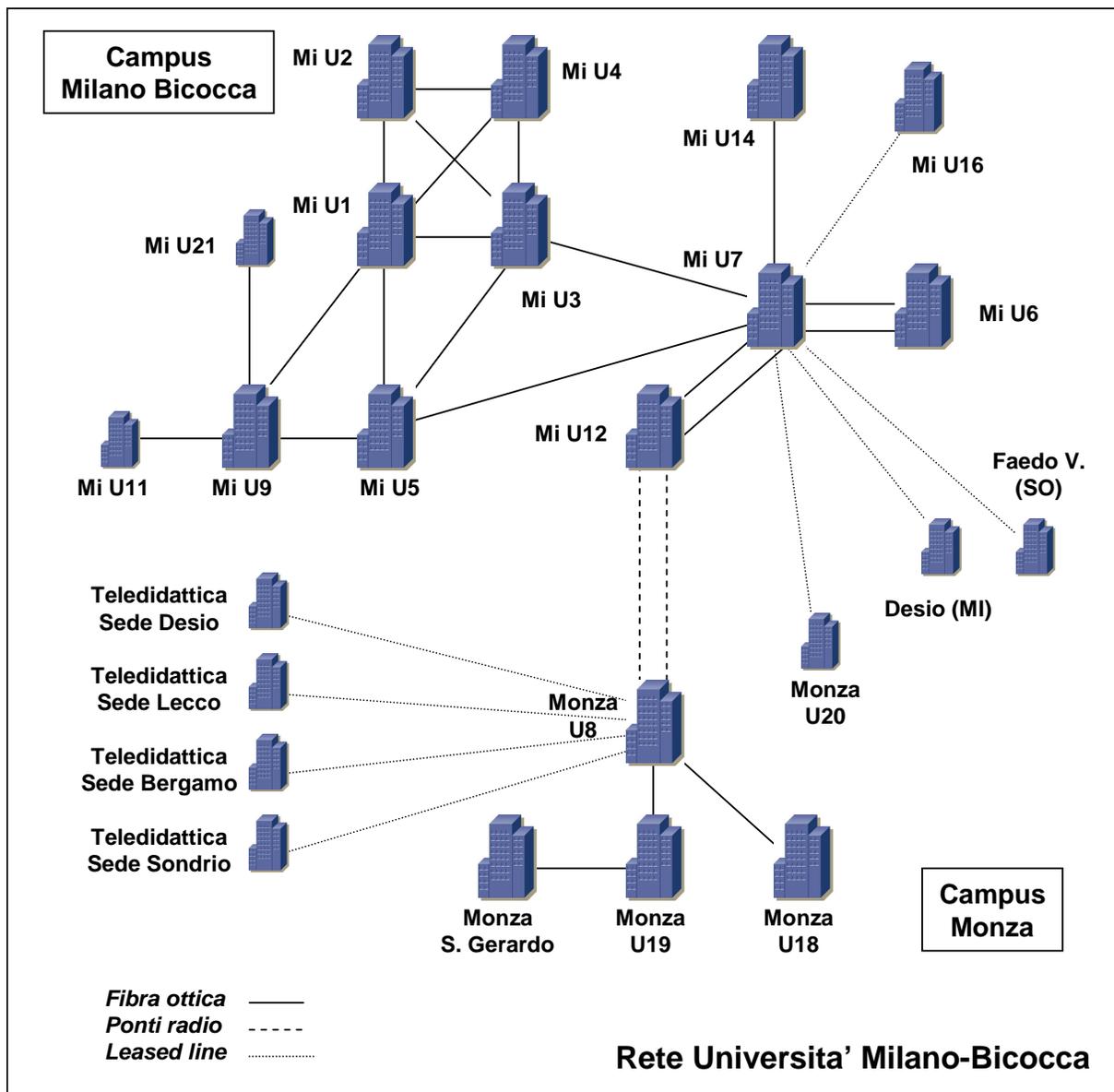


Fig. 1 Rete Università Milano-Bicocca: collegamenti fisici.

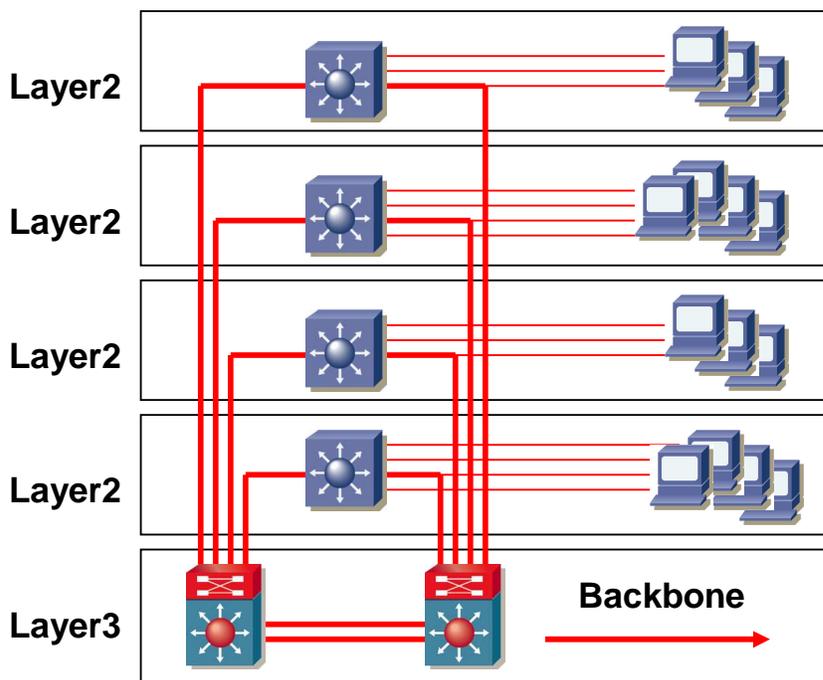


Fig. 2 Distribuzione interna agli edifici.

Protocolli ed indirizzamento

- Nella Rete di Ateneo gli unici protocolli garantiti e permessi sono quelli appartenenti alla suite TCP/IP. Le classi di indirizzamento IP utilizzabili, previo autorizzazione dei Sistemi Informativi, sono:
 - 149.132.0.0/16 (indirizzamento unicast pubblico)
 - 172.17.0.0/16 (indirizzamento unicast privato)
 - 10.0.0.0/8 (indirizzamento unicast privato)
 - 224.0.1.0-238.255.255.255 (multicast global-scope)
 - 239.0.0.0-239.255.255.255 (multicast local-scope)
- Ad ogni Utente che ne fa richiesta viene assegnata, tramite il referente informatico, una postazione di rete con indirizzo IP secondo le modalità del presente regolamento.
- L'Amministratore di Sistema di Ateneo è l'unico responsabile dell'assegnazione e della gestione degli indirizzi IP, che vengono assegnati per i singoli Utenti su richiesta del Referente informatico di struttura tramite apposita modulistica disponibile in formato elettronico sulle pagine web dei Sistemi Informativi.
- L'indirizzo IP è personale e non cedibile; il singolo Utente interno è responsabile dell'uso dell'indirizzo IP assegnato ed è tenuto a comunicarne al Referente informatico di struttura l'eventuale dismissione.

- L'autoassegnazione dell'indirizzo IP è espressamente vietata; l'Utente interno sarà personalmente responsabile della trasgressione al Regolamento.
- Per i Sistemi in Rete su cui possono operare più Utenti deve essere nominato un responsabile al quale verrà assegnato l'indirizzo IP; tale responsabile dovrà garantire la conservazione dei dati necessari all'identificazione dell'Utente utilizzatore in ogni istante di collegamento alla Rete di Università.
- Per i Sistemi in Rete ad utilizzo non personale, purché i soggetti siano quelli autorizzati dalle normative e regolamenti vigenti, ivi compresi gli studenti, deve essere nominato un responsabile del Sistema stesso.
- Anche nei due casi sopra elencati è compito del Referente informatico di struttura richiedere all'Amministratore di Sistema di Ateneo gli indirizzi IP e mantenere aggiornato l'elenco degli stessi con i corrispondenti utenti o responsabili.
- Al fine di garantire la sicurezza informatica, tutte le aree attrezzate per fini didattici o per servizi comunque rivolti agli studenti o al pubblico, quali ad esempio i laboratori e le aule informatiche, devono accedere alla rete tramite un sistema, ad esempio un firewall con funzioni di NAT, che si frapponga tra le postazioni utente (con indirizzi IP privati) ed il resto della rete. A tale scopo deve essere identificabile, per ciascuna delle aree attrezzate, un responsabile con le stesse funzioni e responsabilità del Referente informatico di struttura.

PRINCIPALI SERVIZI

Sicurezza

Tutti i sistemi in rete devono essere mantenuti costantemente in adeguate condizioni di sicurezza. L'Amministratore di Sistema di Ateneo, in quanto responsabile amministrativo e tecnico dei domini (unimib.it, unimib.eu) e dello spazio di indirizzamento IP (149.132.0.0/16) assegnati dalle autorità competenti nazionali ed internazionali deve garantire costantemente il rispetto di tutte le leggi e i regolamenti vigenti, in particolare quelle che riguardano la sicurezza e gli "incidenti" informatici.

A tale scopo le Strutture che intendono offrire servizi informatici attraverso server in rete (web server, ftp server, smtp server, dns server, ecc.) sono tenute a segnalarli preventivamente all'Amministratore di Sistema di Ateneo, il quale verifica che siano garantite le minime condizioni di sicurezza del servizio di seguito elencate:

- presenza di almeno un referente, con funzioni di gestore dei servizi che garantisca la continuità del servizio stesso e che collabori con il referente informatico della struttura,
- aggiornamento costante del servizio in modo che non sia affetto da "bug" noti che ne potrebbero compromettere la sicurezza informatica (le patch da installare saranno tempestivamente comunicate dall'Amministratore di Sistema di Ateneo),
- monitoraggio e **conservazione** per il periodo previsto dalle normative e comunque non inferiore a **5 anni** della registrazione degli accessi al servizio (**file di log**) in modo da consentire all'Amministratore di Sistema di Ateneo eventuali indagini interne o richieste dalle Autorità esterne in caso di uso improprio delle risorse,

- assicurazione verso l'utenza che dette registrazioni non sono disponibili ad alcuno se non nei casi di emergenza riconosciuti come tali dall'Amministratore di Sistema di Ateneo, nel rispetto della normativa vigente sulla "Tutela dei dati personali",

La notifica di un servizio di rete da attivare presso una Struttura va inoltrata all'Amministratore di sistema di Ateneo, secondo le norme da esso definite, sottoscritta dal Responsabile della Struttura stessa e deve obbligatoriamente contenere i seguenti dati:

- descrizione del servizio;
- caratteristiche tecniche del server che fornirà il servizio (Sistema Operativo, indirizzo IP, nome e dominio corrispondenti, nome e versione dell'applicazione).

L'Amministratore di sistema di Ateneo, dopo aver valutato la richiesta, risponderà comunicando in dettaglio le misure di sicurezza da adottare per il particolare servizio.

Il Referente informatico della Struttura che ospita il servizio è tenuto a segnalare immediatamente all'Amministratore di sistema di Ateneo intrusioni o tentativi di intrusione che abbiano avuto come oggetto l'elaboratore che eroga il servizio stesso, mettendo a disposizione i dati delle registrazioni descritte al punto sopra.

Nel caso in cui, a seguito di controlli, segnalazioni o incidenti, l'Amministratore di Sistema di Ateneo rilevi l'inadeguatezza di sistema/servizio per quanto riguarda la sicurezza diretta o indiretta, detto sistema/servizio dovrà essere immediatamente adeguato, secondo le indicazioni fornite dall'Amministratore di Sistema di Ateneo, o staccato dalla rete a cura della Struttura di appartenenza. In difetto dell'azione da parte della Struttura, o nel caso in cui il servizio non sia stato autorizzato, l'Amministratore di Sistema di Ateneo mette in atto tutti gli accorgimenti tecnici ad esso disponibili per disattivare ogni trasporto sulla rete d'Università relativo al sistema inadeguato, sino all'intervento correttivo operato dalla Struttura.

DNS (Domain Name System)

All'Amministratore di Sistema di Ateneo è stata delegata dalle autorità competenti nazionali ed internazionali la gestione amministrativa e tecnica dei domini di secondo livello "unimib.it", "unimib.eu" e dello spazio di indirizzamento IP corrispondente alla rete di classe B 149.132.0.0/16, assegnati all'Università degli Studi di Milano-Bicocca.

Poiché le zone Internet degli indirizzi IP e dei domini hanno una struttura gerarchica ad albero rovesciato, l'Amministratore di Sistema di Ateneo è l'unico responsabile delle zone Internet assegnate all'Università degli Studi di Milano-Bicocca e di tutte quelle sottostanti (sottoreti del tipo "149.132.X/netmask" e sottodomini "zzz.unimib.it", "zzz.unimib.eu").

È compito quindi dell'Amministratore di Sistema di Ateneo garantire in ogni momento il corretto funzionamento delle zone di sua competenza, definendo i sottodomini, gli alias, etc, in modo che ogni computer direttamente connesso alla Rete d'Università o in generale ogni sistema in rete abbia un indirizzo IP e un corrispondente indirizzo Internet (nome di dominio) univoco, statico e registrato nel Domain Name System di Internet.

Il dominio “unimib.it” è suddiviso in sottodomini, normalmente uno per struttura, del tipo “xxx.unimib.it” dove “xxx” è una stringa che rappresenta il nome della struttura stessa (dipartimento, area dell’amministrazione, etc).

La costituzione di un nuovo dominio va richiesta all’Amministratore di Sistema di Ateneo dal responsabile della Struttura a cui si riferisce tramite apposita modulistica disponibile in formato elettronico sulle pagine web dei Sistemi Informativi.

Ogni sistema in rete deve avere un unico indirizzo IP ed un corrispondente nome Internet nel sottodominio della struttura di appartenenza; l’indirizzo IP viene assegnato dall’Amministratore di Sistema di Ateneo al Referente informatico della struttura che lo ha in precedenza richiesto compilando l’apposita modulistica disponibile in formato elettronico sulle pagine web dei Sistemi Informativi in cui vengono forniti alcuni dati tecnici tra cui il nome Internet associato.

È compito del Referente informatico consegnare la coppia “indirizzo IP - nome logico DNS” all’Utente interno finale e **mantenere aggiornata**, con uno storico di almeno **5 anni**, **la lista delle terne “indirizzoIP – nome logico - Utente” assegnati alla sua struttura**, comunicando tempestivamente all’Amministratore di Sistema di Ateneo ogni variazione.

Anche per quanto riguarda l’utilizzo di alias e record MX all’interno del sottodominio di struttura è il Referente informatico che deve richiederne l’attivazione all’Amministratore di Sistema di Ateneo.

Solo i server d’ateneo, cioè quelli che forniscono i servizi con rilevanza di campus (mailserver, web,...) possono appartenere al dominio “unimib.it”.

In casi particolari, da valutare volta per volta, l’Amministratore di Sistema di Ateneo può delegare al Referente informatico la gestione tecnica delle zone relative ai sottodomini e alle sottoreti che riguardano la sua struttura. In questo caso la struttura dovrà dotarsi di un server DNS locale con funzioni di server primario per le zone delegate di cui il server DNS d’ateneo farà da secondario.

L’Amministratore di Sistema di Ateneo, che rimane comunque il solo responsabile amministrativo e tecnico rispetto alle autorità competenti nazionali ed internazionali, concorderà con la struttura delegata le modalità di gestione tecnico-amministrativa e di sicurezza del servizio e controllerà che ne vengano rispettate le condizioni.

In caso di violazione alle norme sopra esposte, in particolare in caso di attività di rete di un sistema in rete non registrato nel DNS e quindi non autorizzato, l’Amministratore di Sistema di Ateneo provvederà ad adottare le misure più idonee a sua disposizione, a seconda della gravità dell’infrazione.

Autenticazione di Ateneo

L’Università mette a disposizione un sistema centralizzato di autenticazione basato su un directory server LDAP contenente i dati utente, il suo username, la sua password ed i servizi ai quali esso ha accesso.

I servizi sotto autenticazione ai quali l'utente ha accesso all'attivazione del proprio profilo sono: posta elettronica, servizio di cambio password, visualizzazione cedolini on-line, accesso rete wireless, accesso banche dati on-line, accesso remoto e, per i docenti, accesso rete aule didattiche.

Condizione necessaria per l'attivazione è che l'utente appartenga al personale strutturato dell'Ateneo oppure, in caso di persona fisica non strutturata, l'attivazione avviene a seguito di autorizzazione da parte del proprio Responsabile di Struttura o di un suo delegato, previa registrazione dei dati identificativi e sottoscrizione del modulo di autorizzazione al trattamento dei dati personali.

L'Amministratore di Sistema di Ateneo ne assicura in modo esclusivo la gestione, la riservatezza, il monitoraggio, la sicurezza e l'aggiornamento secondo le regole da esso definite.

L'Utente interno autorizzato è personalmente responsabile del mantenimento della necessaria riservatezza sui propri codici d'accesso e/o sulle proprie password come specificato nel presente regolamento.

Ogni servizio al quale l'utente ha accesso è subordinato all'accettazione, da parte dell'utente stesso, del presente regolamento.

In particolare la coppia username e password utente è unica e garantisce l'accesso ad ogni tipo di dati personali e servizi dell'utente.

Posta elettronica d'Ateneo

L'Amministratore di sistema d'Ateneo gestisce il mail server d'ateneo con indirizzi del tipo identificativo@unimib.it, dove "identificativo" è generalmente "nome.cognome" dell'Utente nel caso di casella di posta personale o "nomestruttura" per le caselle che fanno riferimento ad una struttura o ad un servizio.

Ciascuna Struttura viene dotata d'ufficio di un indirizzo di posta elettronica del tipo "referente-informatico-struttura@unimib.it" al quale verranno validamente inviate le comunicazioni da parte dell'Amministratore di sistema d'Ateneo ai referenti informatici.

L'Amministratore di Sistema di Ateneo ne assicura in modo esclusivo la gestione, il monitoraggio, la sicurezza, l'aggiornamento e la pubblicizzazione secondo le regole da esso definite.

Le caselle sono strettamente personali, le password di accesso non cedibili; anche nel caso di caselle di struttura deve esserci un responsabile per cui valgono le stesse regole.

Collegato al servizio di posta elettronica è attivo un servizio di antivirus e antispam che filtra le e-mail in entrata ed in uscita dal dominio dell'Università mettendo in quarantena quelle sospette ed eliminando eventuali virus.

L'Utente ha accesso ad una pagina web per l'amministrazione e la personalizzazione della propria casella di posta elettronica e per la visione delle e-mail sospette messe in quarantena.

È possibile accedere alla propria casella di posta elettronica in due modi: tramite un client di posta opportunamente configurato o per mezzo di un web browser.

L'Utente prende atto dell'esistenza del registro dei collegamenti e delle attività (log) che verrà custodito dall'Amministratore di sistema d'Ateneo per gli usi e gli scopi consentiti dalla Legge e dai Regolamenti dell'Ateneo.

Le strutture universitarie che intendano dotarsi di un proprio servizio di posta elettronica, con indirizzo del tipo "identificativo@sottodominio.unimib.it", dovranno attivare e gestire il servizio locale garantendo tutte le condizioni di sicurezza del servizio e il rispetto della normativa vigente.

Inoltre tutte le strutture autorizzate possono richiedere all'Amministratore di Sistema di Ateneo, secondo una procedura stabilita, l'inoltro di messaggi di posta elettronica, con mittente l'indirizzo della struttura stessa o di un suo rappresentante, a tutti gli utenti o a particolari aree di utenza del mailserv d'ateneo.

Accesso rete wireless

L'Università mette a disposizione degli utenti autorizzati un servizio di accesso wireless alla rete di Ateneo. L'accesso a tale servizio è vincolato al possesso di un certificato personale rilasciato dalla Certification Authority d'Ateneo tramite procedura web su canale sicuro autenticato.

L'accesso a tale procedura avviene tramite i diritti e le credenziali dell'utente derivate dal sistema di autenticazione di Ateneo.

L'Amministratore di Sistema di Ateneo assicura in modo esclusivo la gestione, il monitoraggio, la sicurezza e l'aggiornamento dell'infrastruttura a chiave pubblica (PKI) secondo le regole da esso definite.

L'Utente si fa carico della corretta configurazione del proprio computer e dell'installazione del software necessario al collegamento, secondo le specifiche che gli verranno fornite.

Il servizio è strettamente personale e legato all'utilizzo del certificato, che dovrà pertanto essere custodito con la massima cura e riservatezza dall'utente stesso, che può in qualsiasi momento richiederne la revoca. L'Utente si assume la responsabilità di ogni uso improprio dello stesso.

L'Utente si impegna esplicitamente al rispetto di ogni norma o regolamento che disciplini l'utilizzo della Rete all'interno dell'Ateneo.

L'Utente ha l'obbligo di comunicare immediatamente la perdita dei requisiti necessari, impegnandosi a cessare immediatamente l'utilizzo del servizio.

L'Università si riserva il diritto di sospendere o revocare in qualsiasi momento senza preavviso l'autorizzazione all'accesso al servizio; in tale caso verrà data comunicazione all'Utente tramite e-mail alla casella di posta presso il server di Ateneo.

L'Utente prende atto dell'esistenza del registro dei collegamenti e delle attività (log) che verrà custodito dall'Amministratore di sistema d'Ateneo per gli usi e gli scopi consentiti dalla Legge e dai Regolamenti dell'Ateneo.

Accesso banche dati on-line

L'Università mette a disposizione degli utenti autorizzati un servizio di accesso alle banche dati on-line della Biblioteca di Ateneo da reti esterne alla rete di Ateneo tramite un proxy server. L'accesso al servizio avviene tramite i diritti e le credenziali dell'utente derivate dal sistema di autenticazione di Ateneo.

L'Utente si fa carico della corretta configurazione del proprio computer e dell'installazione del software necessario al collegamento, secondo le specifiche che gli verranno fornite.

Il servizio è strettamente personale e legato all'utilizzo dell'identificativo e della password, che dovrà pertanto essere custodita con la massima cura e riservatezza. L'Utente si assume la responsabilità di ogni uso improprio della stessa.

L'Utente si impegna esplicitamente al rispetto di ogni norma o regolamento che disciplini l'utilizzo della Rete all'interno dell'Ateneo.

L'Utente ha l'obbligo di comunicare immediatamente la perdita dei requisiti necessari, impegnandosi a cessare immediatamente l'utilizzo del servizio.

L'Università si riserva il diritto di sospendere o revocare in qualsiasi momento senza preavviso l'autorizzazione all'accesso al servizio; in tale caso verrà data comunicazione all'Utente tramite e-mail alla casella di posta presso il server di Ateneo.

L'Utente prende atto dell'esistenza del registro dei collegamenti e delle attività (log) che verrà custodito dall'Amministratore di sistema d'Ateneo per gli usi e gli scopi consentiti dalla Legge e dai Regolamenti dell'Ateneo.

Accesso rete aule didattiche

L'Università mette a disposizione degli utenti autorizzati un servizio di accesso alla rete cablata nelle aule didattiche tramite protocollo 802.1X.

L'accesso a tale servizio è vincolato al possesso di un certificato personale rilasciato dalla Certification Authority d'Ateneo tramite procedura web su canale sicuro autenticato.

L'accesso a tale procedura avviene tramite i diritti e le credenziali dell'utente derivate dal sistema di autenticazione di Ateneo.

L'Amministratore di Sistema di Ateneo assicura in modo esclusivo la gestione, il monitoraggio, la sicurezza e l'aggiornamento dell'infrastruttura a chiave pubblica (PKI) secondo le regole da esso definite.

L'Utente si fa carico della corretta configurazione del proprio computer e dell'installazione del software necessario al collegamento, secondo le specifiche che gli verranno fornite.

Il servizio è strettamente personale e legato all'utilizzo del certificato, che dovrà pertanto essere custodito con la massima cura e riservatezza dall'utente stesso, che può in qualsiasi momento richiederne la revoca. L'Utente si assume la responsabilità di ogni uso improprio dello stesso.

L'Utente si impegna esplicitamente al rispetto di ogni norma o regolamento che disciplini l'utilizzo della Rete all'interno dell'Ateneo.

L'Utente ha l'obbligo di comunicare immediatamente la perdita dei requisiti necessari, impegnandosi a cessare immediatamente l'utilizzo del servizio.

L'Università si riserva il diritto di sospendere o revocare in qualsiasi momento senza preavviso l'autorizzazione all'accesso al servizio; in tale caso verrà data comunicazione all'Utente tramite e-mail alla casella di posta presso il server di Ateneo.

L'Utente prende atto dell'esistenza del registro dei collegamenti e delle attività (log) che verrà custodito dall'Amministratore di sistema d'Ateneo per gli usi e gli scopi consentiti dalla Legge e dai Regolamenti dell'Ateneo.

Accesso remoto

L'Università mette a disposizione degli utenti autorizzati un servizio di accesso remoto (RAS) che permette la connessione alla Rete d'Ateneo di postazioni utente per mezzo di modem analogici o ISDN.

L'accesso al servizio avviene tramite i diritti e le credenziali dell'utente derivate dal sistema di autenticazione di Ateneo.

L'Amministratore di Sistema di Ateneo ne assicura in modo esclusivo la gestione, il monitoraggio, la sicurezza e l'aggiornamento secondo le regole da esso definite.

L'Utente si fa carico della corretta configurazione del proprio computer e dell'installazione del software necessario al collegamento, secondo le specifiche che gli verranno fornite.

Il servizio è strettamente personale e legato all'utilizzo dell'identificativo e della password, che dovrà pertanto essere custodita con la massima cura e riservatezza. L'Utente si assume la responsabilità di ogni uso improprio della stessa.

L'Utente si impegna esplicitamente al rispetto di ogni norma o regolamento che disciplini l'utilizzo della Rete all'interno dell'Ateneo.

L'Utente ha l'obbligo di comunicare immediatamente la perdita dei requisiti necessari, impegnandosi a cessare immediatamente l'utilizzo del servizio.

L'Università si riserva il diritto di sospendere o revocare in qualsiasi momento senza preavviso l'autorizzazione all'accesso al servizio; in tale caso verrà data comunicazione all'Utente tramite e-mail alla casella di posta presso il server di Ateneo.

L'Utente prende atto dell'esistenza del registro dei collegamenti e delle attività (log) che verrà custodito dall'Amministratore di sistema d'Ateneo per gli usi e gli scopi consentiti dalla Legge e dai Regolamenti dell'Ateneo.

Servizi agli studenti

L'Università mette a disposizione un sistema centralizzato di autenticazione basato su un directory server LDAP contenente i dati dello studente, il suo username, la sua password ed i servizi per i quali è autorizzato.

I servizi sotto autenticazione ai quali lo studente ha accesso all'attivazione del proprio profilo, creato all'atto dell'iscrizione all'Università, sono: posta elettronica (n.cognome<N>@campus.unimib.it, servizio di cambio password, accesso banca dati carriere SIFA on-line, accesso rete wireless e accesso banche dati on-line.

I servizi agli studenti sono erogati con le stesse modalità e gli stessi vincoli di quelli per il personale dell'Università oggetto di questo allegato e per i quali si intende l'accettazione del presente regolamento.

L'Amministratore di Sistema di Ateneo ne assicura in modo esclusivo la gestione, la riservatezza, il monitoraggio, la sicurezza e l'aggiornamento secondo le regole da esso definite.

Lo studente viene equiparato all'Utente interno ed è personalmente responsabile delle attività riconducibili alla sua identità ai sensi del regolamento di Rete di Ateneo dell'Università degli Studi di Milano Bicocca.

Lo studente è personalmente responsabile del mantenimento della necessaria riservatezza sui propri codici d'accesso e/o sulle proprie password come specificato nel presente regolamento.

In particolare la coppia username e password dello studente è unica e garantisce l'accesso ad ogni tipo di dati personali e servizi a lui forniti.

Ogni servizio al quale lo studente ha accesso è subordinato all'accettazione, da parte dello studente stesso, del presente regolamento.

RETE FONIA

Descrizione sistema fonia.

Il sistema di fonia di Ateneo, facente capo alla radice 02 6448, è costituito da un sistema distribuito composto da un centro stella dislocato nell'edificio U7 (comprendente anche i servizi di "caselle vocali" e di accounting centralizzati) e, ad esso collegati, uno o più satelliti collocati presso vari edifici dell'Ateneo. La tecnologia utilizzata è basata su centralini convenzionali (PABX con protocollo QSIG), per la dorsale di campus, integrati con zone VoIP (Voice over IP) per le sedi remote.

L'uscita e l'entrata delle chiamate viene assicurata da flussi distribuiti nel centro stella e nei vari satelliti secondo uno schema di bilanciamento ottimizzato in base al traffico.

Il sistema di fonia d'Ateneo utilizza per la distribuzione il cablaggio strutturato realizzato per la Rete d'Ateneo, e pertanto ne assume le definizioni e le norme previste dal presente regolamento.

Il sistema è basato su collegamenti digitali e l'uso delle eventuali linee analogiche è riservato all'utilizzo di fax. È espressamente vietato il collegamento di apparecchiature attive o passive non rispondenti alle caratteristiche tecniche richieste dalla specifica attivazione della singola "presa utente", richiedibili all'Amministratore di sistema di Ateneo, potendo comportare anche danneggiamenti al sistema di fonia di Ateneo ed agli stessi dispositivi collegati.

Tutti gli apparati "telefono" vengono forniti dall'Amministratore di sistema d'Ateneo per garantirne la compatibilità con il sistema digitale e la centralità di gestione del sistema di fonia di Ateneo.

È cura del Responsabile della Struttura riconoscere il singolo numero telefonico assegnato, autorizzandone l'attivazione da parte dell'Amministratore di sistema di Ateneo, come appartenente al proprio centro di costo; ne assicura la correttezza dell'utilizzazione qualora accessibile da parte di più persone fisiche; è cura del singolo Utente comunicare ogni variazione della propria situazione all'Amministratore di sistema d'Ateneo, verificandone inoltre la correttezza nella rubrica on-line di Ateneo.

Data la criticità del servizio è l'Amministratore di Sistema di Ateneo che ne assicura in modo esclusivo la gestione, il monitoraggio, la sicurezza, l'aggiornamento e la pubblicizzazione secondo le regole da esso definite.

È vietata, all'interno del Campus, l'attivazione di singole linee o di sistemi di fonia esterni al sistema di fonia di Ateneo, fatta salva un'espressa autorizzazione da parte dell'Amministratore di sistema di Ateneo per eccezionali e comprovate esigenze. Ogni attivazione di singole linee o di sistemi di fonia esterni al Campus ma riconducibili all'Ateneo deve essere comunicata tempestivamente all'Amministratore di sistema d'Ateneo ed agli Organi Contabili dell'Ateneo.

È espressamente vietato l'accesso remoto alla Rete dell'Università se non tramite l'apposito servizio messo a disposizione dall'Amministratore di sistema di Ateneo.

DISPOSIZIONI OPERATIVE PER I SITI WEB D'ATENEO

Il portale di Ateneo (www.unimib.it) contiene al suo interno informazioni generali sull'Ateneo (organizzazione generale della didattica, della ricerca e dell'amministrazione centrale; organi di governo; informazioni logistiche, ecc.). Inoltre contiene le schede dei docenti e ricercatori interni all'Ateneo.

Il portale è gestito dall'Ufficio Redazione Web, che definisce e mantiene la corretta organizzazione dei contenuti informativi del sito. Le Strutture responsabili di tali contenuti (Facoltà, Dipartimenti, Centri, Aree e Uffici dell'Amministrazione), se lo desiderano, possono gestire direttamente l'inserimento e l'aggiornamento dei contenuti, utilizzando le funzioni di supporto alla redazione messe a disposizione dal portale. In tal caso, l'Ufficio Redazione Web assegna i diritti d'accesso alle varie sezioni del sito, e fornisce il necessario supporto ai redattori (formazione e risoluzione di problemi). L'Ufficio Redazione Web assicura l'aggiornamento dei contenuti di quelle sezioni del sito che non sono gestite da altri Enti o Strutture.

Le schede dei docenti e ricercatori dell'Ateneo potranno essere aggiornate direttamente dagli interessati, o dall'Ufficio Redazione Web, in particolari occasioni. In tal caso, l'Ufficio provvederà a richiedere agli interessati le informazioni aggiornate.

Il portale di Ateneo risiede su elaboratori gestiti dall'Amministratore di sistema di Ateneo (Area Sistemi Informativi), che provvede, in particolare, a gestire il dominio "unimib.it" e lo spazio di indirizzamento IP assegnato all'Ateneo, e tutti gli aspetti di natura sistemistica del portale (sicurezza, backup, continuità del servizio).

Per motivi di sicurezza della rete di Ateneo, le informazioni contenute nel portale possono essere aggiornate esclusivamente con le funzioni messe a disposizione a tal scopo dal portale stesso.

I siti delle Facoltà e dei Dipartimenti (comprendenti, in particolare quanto attiene all'attività didattica e di ricerca facenti capo a tali strutture), sono raggiungibili dal portale di Ateneo attraverso appositi collegamenti, ma sono esterni ad esso. Questi siti sono gestiti autonomamente dalle strutture interessate, sia per quanto riguarda l'aggiornamento dei contenuti, sia per quanto riguarda la infrastruttura sistemistica che li ospita.

Le Facoltà e i Dipartimenti possono richiedere l'assegnazione di nomi del tipo:

www.<Dip/Fac>.unimib.it

secondo le modalità descritte nel Regolamento della rete di Ateneo.

Esempi: www.medicina.unimib.it (Facoltà di Medicina)
www.psicologia.unimib.it (Facoltà di Psicologia)
www.scienze.unimib.it (Facoltà di Scienze)

www.btbs.unimib.it
www.dimequant.unimib.it
www.disco.unimib.it

(Dipartimento di Biotecnologie e Bioscienze)
(Dipartimento di Metodi Quantitativi)
(Dip. di Informatica, sistemistica e Comunicazione)

Allo scopo di facilitare la reperibilità delle informazioni da parte degli utenti, e per una migliore gestione da parte dell'Area Sistemi Informativi, è necessario evitare una eccessiva proliferazione di nomi concepiti con modalità eterogenee. È in corso una razionalizzazione, ove possibile, delle situazioni pregresse. Per i nomi da assegnare in futuro, ci si atterrà ai seguenti criteri generali.

1. Nel caso di siti dedicati a laboratori, progetti, iniziative, pubblicazioni, o, in generale, iniziative facenti capo a una Facoltà o a un Dipartimento, dovranno essere utilizzati nomi del tipo:

www.<iniziativa>.<Dip/Fac>.unimib.it

Esempi: www.lta.disco.unimib.it (Laboratorio di Test e Analisi del software del Dipartimento di Informatica, Sistemistica e Comunicazione)

2. Nel caso di iniziative afferenti direttamente all'Ateneo o di iniziative congiunte fra più Dipartimenti o Facoltà, potranno essere proposti nomi del tipo

www.<iniziativa>.unimib.it

Questi casi dovranno essere singolarmente approvati dal Rettore, o dal Coordinatore Web di Ateneo (Prof. Roberto Polillo), sulla base di una richiesta motivata.

Esempi: www.indam.unimib.it (Ist.Nazionale di alta Matematica – sezione di Milano)
www.nomadis.unimib.it (progetto interdipartimentale)
www.plasmaprometeo.unimib.it (Centro di eccellenza sui plasmi)
www.nettuno.unimib.it (Foro Tecnologico Nettuno)

3. Si raccomanda di ridurre al minimo la richiesta di nomi sinonimi riferentisi allo stesso sito (alias)

4. Per quanto riguarda la didattica, il portale www.unimib.it contiene informazioni di carattere generale sulla offerta didattica dell'Ateneo, gestite dall'amministrazione centrale e rinnovate con cadenza annuale. Per quanto riguarda le informazioni relative alle attività didattiche dei vari corsi di studio (corsi di laurea, laurea specialistica, master, corsi di perfezionamento, scuole di specializzazione e dottorati di ricerca), esse sono gestite autonomamente dalle Facoltà e/o Dipartimenti coinvolti, sia per quanto riguarda i contenuti informativi sia per quanto riguarda

l'infrastruttura sistemistica. Si fa presente che, per i corsi di studio, in considerazione del loro elevato numero, non verranno assegnati nomi individuali (cioè del tipo www.<corso>.unimib.it). Per quanto riguarda i master, può essere anche richiesta l'assegnazione di un nome del tipo:

www.<siglamaster>.master.unimib.it

5. In nessun caso, per motivi relativi alla organizzazione sistemistica dei server del portale, potranno essere autorizzati nuovi nomi della forma:

www.unimib.it/<nome>

Le richieste di nomi devono essere inoltrate all'Area Sistemi Informativi, che provvederà a richiedere, ove necessario, l'autorizzazione al Rettore o al Coordinatore Web di Ateneo. La modulistica per la richiesta è reperibile alla sezione regolamenti del portale di Ateneo (<http://www.unimib.it>).

Per quanto non specificato qui sopra, si fa riferimento al "Regolamento relativo all'accesso e all'utilizzazione della rete informatica e telematica dell'Università".

Assegnazione nomi per siti web d'Ateneo

MODULO di RICHIESTA

Al Responsabile dell'Area Sistemi Informativi

da inviare a: sistemi@unimib.it

Data della richiesta:

Dati del richiedente:

Nome:

Cognome:

Struttura:

Ruolo:

e-mail:

telefono:

Nome del sito web richiesto (si veda Regolamento):

Motivazione della richiesta:

Strutture coinvolte

Nome del responsabile amministrativo del sito (se diverso dal richiedente):

Dati tecnici del server che ospita il portale (Indirizzo IP, Collocazione, ...)

Nome del referente informatico di riferimento:

Data di Scadenza (da indicare nel caso di progetti a termine):

Come da regolamento, il richiedente dichiara di assumersi la responsabilità degli eventuali abusi che possano essere commessi, anche da terzi non utenti interni, attraverso i servizi sopra indicati.

DISPOSIZIONI OPERATIVE PER L'ACCESSO ALLA RETE D'ATENEO DALLE AREE ATTREZZATE PER SERVIZI RIVOLTI AGLI STUDENTI O AL PUBBLICO (LABORATORI INFORMATICI)

La realizzazione di aree attrezzate per fini didattici o per servizi comunque rivolti agli studenti o al pubblico, come ad esempio i laboratori e le aule informatiche, prevede l'aderenza ai relativi standard vigenti in Ateneo.

In particolare per ciascun laboratorio viene creata una rete distinta, separata ed isolata dal resto della rete d'Ateneo.

I Sistemi Informativi assegnano a ciascun laboratorio un insieme di indirizzi IP privati, utilizzabili esclusivamente per quel laboratorio, da cui vengono ricavati gli indirizzi IP da assegnare alle postazioni interne al laboratorio stesso.

I primi 16 IP dell'insieme di indirizzi assegnati sono riservati ai Sistemi Informativi, per cui, in caso venga assegnato un blocco di 256 IP, gli indirizzi disponibili sono compresi nell'insieme che va dall'indirizzo 172.17.xxx.17 all'indirizzo 172.17.xxx.254 inclusi.

Al fine di garantire il rispetto dei livelli minimi di sicurezza, l'accesso dalle postazioni interne al laboratorio a risorse disponibili all'esterno dello stesso è permesso solo attraverso un firewall con funzioni di NAT/PAT che si frapponga tra la rete del laboratorio ed il resto della rete d'Ateneo.

La Security Policy comune a tutti i laboratori, attualmente vigente, salvo fatto il diritto di ciascuna struttura di adottarne di più severa, prevede che attraverso il firewall possano passare esclusivamente i seguenti protocolli:

SMTTP/SMTPS, POP3/POP3S, IMAP4/IMAP4S, HTTP/HTTPS.

E' inoltre obbligatorio che l'interfaccia esterna del firewall risponda alle richieste ICMP di echo replay provenienti da macchine con IP sorgente appartenete alla rete 149.132.0.0/16.

La Security Policy prevede inoltre che l'uso delle postazioni da parte di ciascun utente è consentito solo previa autenticazione; per tale motivo ogni utente deve avere un account personale e non cedibile (protetto da una password) e deve essere identificabile e riconoscibile.

I **log** con i dati necessari ad identificare chi tra i vari utenti autorizzati usava una postazione in un dato istante (ore, minuti, secondi, giorno, mese, anno) **vanno conservati** per un periodo non inferiore a **5 anni**.

E' caldamente consigliato che ciascun laboratorio adotti un proprio regolamento d'uso che deve essere conosciuto e rispettato dagli utenti al pari del regolamento d'Ateneo e della User Policy del GARR che ne costituisce parte integrante nel suo ambito di applicazione.

Per ciascun laboratorio deve essere nominato un responsabile (tecnico ed amministrativo) che ha l'obbligo di mettere in pratica tutti gli accorgimenti sopra menzionati e risponde delle eventuali mancanze.

E' lasciata alla discrezionalità delle singole strutture, purchè ne venga data comunicazione ufficiale ai Sistemi Informativi, la possibilità di nominare un responsabile amministrativo e di delegare la realizzazione e la supervisione tecnica ad un'altra persona (responsabile tecnico).

Tutti gli eventuali avvicendamenti dei responsabili devono essere tempestivamente comunicati in forma ufficiale, dal responsabile amministrativo in carica, ai Sistemi Informativi.

Nella fase di realizzazione del laboratorio il responsabile è tenuto a dichiarare il numero di postazioni client e server presenti nel laboratorio, fornire l'elenco delle prese da attivare sulla rete del laboratorio, evidenziando le prese a cui verranno collegati i server e, limitatamente alla macchina/sistema con funzione di firewall, a segnalare la presa usata per l'interfaccia interna al laboratorio e quella per l'interfaccia esterna.

Per la sola interfaccia esterna del firewall sarà cura del responsabile del laboratorio, tramite il referente informatico, fare richiesta di un indirizzo pubblico.

DISPOSIZIONI OPERATIVE PER GLI APPLICATIVI GESTIONALI IN RETE

Questo documento elenca le norme di conformità alle quali deve soddisfare qualunque applicativo gestionale che utilizzi la rete di Ateneo.

Il funzionamento in rete di tale applicativo dovrà sottostare al pieno rispetto del regolamento di rete di ateneo.

Da ciò consegue, in particolare, la nomina di un responsabile, interno all'ateneo, delle macchine coinvolte (*e che quindi ne sarà amministratore*) che opererà come interfaccia verso i Sistemi Informativi sia nella fase di realizzazione del progetto sia nella sua gestione.

Il responsabile interno, compatibilmente al regolamento di rete di ateneo, dovrà mantenere le macchine aggiornate al migliore livello di sicurezza possibile e dovrà collaborare con l'entità manuttrice dell'applicativo in quanto unico depositario della password di amministratore del sistema.

Software:

- L'applicativo deve avere le caratteristiche adeguate ad un uso in rete; deve in particolar modo utilizzare il minor numero possibile di porte di rete (se utilizza il modello client-server le porte sulle quali il lato server è in ascolto devono essere fisse) e girare come servizio (non è quindi necessario login, automatico e non, dell'utente owner dell'applicativo per avviare il servizio che questo svolge).
- L'applicativo deve prevedere un "superutente" con compiti di amministrazione (che non deve essere comunque amministratore del sistema) e utenti di livello più basso, affinché sia possibile creare password e profili blindati per gli utenti non amministratori dell'applicativo e consentire la gestione a norma di regolamento di rete di ateneo dei log delle macchine sulle quali questo è installato.

Nel caso in cui l'applicativo non risponda a queste caratteristiche i Sistemi Informativi si riservano il diritto di valutare, nell'ambito del regolamento di rete di ateneo, se mettere o no in rete le macchine su cui esso è installato.

Monitoraggio da remoto:

- Per consentire interventi da remoto sulle macchine si dovrà prevedere un collegamento RTG con diritti di accesso per utente non amministratore (ciò implica il fatto che ogni intervento che necessiti dei diritti amministrativi del sistema potrà essere effettuato solo in locale).
- La connessione dovrà sempre essere originata dalle macchine presso l'università (la configurazione dell'accesso remoto non dovrà permettere connessioni verso le macchine dall'esterno).

NOTA - La possibilità di utilizzare collegamenti su linee dedicate dovrà essere preventivamente discussa con i Sistemi Informativi.

I Sistemi Informativi si riservano il diritto di decidere, nel caso si ritenesse necessario, l'implementazione di ulteriori politiche di sicurezza nell'architettura di rete sottostante.

DISPOSIZIONI OPERATIVE PER L'ACCESSO ALLA RETE DELLA RESIDENZA UNIVERSITARIA EDIFICIO U12

Servizi di rete offerti

Per ogni ospite è previsto un telefono e un accesso internet.

Le condizioni e le modalità di attivazione del servizio sono vincolate all'accettazione da parte dell'ospite del regolamento di Rete di Ateneo dell'Università degli Studi di Milano Bicocca ⁽¹⁾.

Rete dati/fonia

Per ogni posto letto in ogni stanza della residenza universitaria dell'edificio universitario U12 sono installate due prese utente interne di rete.

Una presa di rete è dedicata all'accesso alla rete di Ateneo ed ha associato un indirizzo IP non modificabile.

All'altra presa di rete è collegato un apparecchio telefonico fornito dall'Università.

All'atto della registrazione l'ospite riceve dal *referente informatico di struttura* ⁽²⁾ un documento (*vedi modulo allegato*) riportante, oltre all'assunzione di responsabilità come *utente interno* ⁽³⁾, il numero di presa di rete, l'indirizzo IP che potrà utilizzare ed il numero di telefono a lui assegnato.

Assunzione di responsabilità

L'utente è personalmente responsabile delle attività riconducibili all'indirizzo IP a lui affidato ai sensi del regolamento di Rete di Ateneo dell'Università degli Studi di Milano Bicocca.

L'unicità dell'indirizzo IP a lui affidato è garantita dall'*Amministratore di Sistema di Ateneo* ⁽⁴⁾.

Si riporta uno stralcio dell'Articolo 4 del Regolamento di Rete:

Articolo 4 - Modalità di accesso alla Rete dell'Università

Per potere accedere alla Rete d'Università ogni Utente interno dovrà ottenere una specifica autorizzazione dal responsabile della struttura di appartenenza.

Per poter connettere un qualunque Sistema in Rete il Referente informatico di struttura deve ottenere una specifica autorizzazione dall'Amministratore di Sistema d'Ateneo che rilascerà un apposito indirizzo IP; il Referente informatico di struttura garantirà la corrispondenza tra l'indirizzo IP e l'Utente interno. L'autoassegnazione dell'indirizzo IP è espressamente vietata.

L'Utente interno otterrà l'autorizzazione all'accesso alla Rete d'Università, anche temporaneamente, soltanto se identificato ed identificabile. A tale scopo, l'Utente acconsentirà al trattamento dei suoi dati personali da parte dell'Ateneo, in conformità alle norme legislative e regolamentari vigenti e applicabili, sottoscrivendo il modulo secondo il facsimile di cui all'allegato 2 al presente Regolamento.

L'Utente interno otterrà l'autorizzazione dopo essersi impegnato ad osservare il presente Regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono per il tramite della Rete d'Università.

L'Utente interno può accedere solo a quei servizi della Rete d'Università per i quali è stato espressamente autorizzato e con le modalità consentite.

(omissis)

L'Utente interno autorizzato è personalmente responsabile del mantenimento della necessaria riservatezza sui propri codici d'accesso e/o sulle proprie password. L'Utente si impegna a comunicare immediatamente al Referente informatico di struttura lo smarrimento, il furto o l'appropriazione da parte di terzi dei propri codici d'accesso e/o delle proprie password.

L'Utente interno è responsabile delle attività svolte nella Rete d'Università attraverso l'utilizzazione dei codici e/o delle password a lui assegnate.

L'Utente interno è tenuto a segnalare immediatamente qualsiasi errore o malfunzionamento della Rete d'Università di cui sia venuto a conoscenza al Referente informatico di struttura, il quale, dopo aver appurato che non si tratti di problemi di sua competenza, deve a sua volta riferirne tempestivamente all'Amministratore del sistema di Ateneo.

Note

(1) <http://www.si.unimib.it/regolamento/regolamento-rete-bicocca.pdf>;

(2) *Referente informatico di struttura*: responsabile amministrativo e tecnico di ogni sistema in rete a valle di una presa utente e dei relativi servizi, nominato dal Responsabile amministrativo della struttura: ISU;

(3) *Utente interno*: qualsiasi persona o struttura autorizzata che acceda alla Rete d'Università;

(4) *Amministratore di sistema di Ateneo*: Area Sistemi Informativi, responsabile della gestione amministrativa e tecnica della rete d'Università, del dominio "unimib.it" e dello spazio di indirizzamento IP 149.132.0.0/16;

PARAMETRI DI CONFIGURAZIONE PER L'ACCESSO ALLA RETE DATI

IP Address: **149.132.X.Y**
Subnet Mask: **255.255.255.0**
Default Gateway: **149.132.X.1**
Primary Dns: **149.132.2.3**
Secondary Dns: **149.132.192.3**

ACCESSO ALLA RETE DI ATENEO DALLE STANZE DELLA RESIDENZA STUDENTI - EDIFICIO U12

Assegnazione dell'indirizzo Ip per l'accesso alla Rete dell'Università degli Studi di Milano – Bicocca ed

Accettazione del Regolamento di utilizzo della rete

MODULO DI AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI

Con la presente il/la Sottoscritto/a _____

residente a _____, in Via _____

nella sua qualità di _____

tel. _____, e-mail _____, matricola _____

Ospite presso l'edificio **U12**, Stanza **N.** _____, Piano **N.** _____, per il periodo dal _____

al _____ **RICEVE** l'autorizzazione ad accedere alla rete dell'Università degli Studi di

Milano – Bicocca tramite l'indirizzo IP: **149.132.** ____ . ____ da utilizzarsi personalmente e

comunque sotto la propria responsabilità da postazioni connesse alla presa dati **N.** _____

DICHIARA

- di avere richiesto l'autorizzazione all'accesso alla Rete d'Università;
- di avere preso visione del Regolamento relativo all'accesso e all'utilizzazione della rete informatica e telematica dell'Università e in particolare dell'Art. 4 - *Modalità di accesso alla Rete dell'Università* del predetto Regolamento;
- di impegnarsi a rispettare in ogni sua parte il predetto Regolamento;
- di essere stato informato che l'espressione del consenso al trattamento dei propri dati personali ha natura facoltativa. Tuttavia, in base all'Art. 4 - *Modalità di accesso alla Rete dell'Università* del predetto Regolamento, la mancata espressione del consenso al trattamento dei dati personali richiesti per l'autorizzazione all'accesso alla Rete d'Università determinerà l'impossibilità di concedere la predetta autorizzazione;
- di essere stato informato, ai sensi dell'art. 13 del D.lgs 196/2003 "Codice in materia di protezione dei dati personali", che i propri dati personali forniti all'atto della compilazione della richiesta di autorizzazione di accesso alla Rete d'Università saranno trattati in conformità alle norme legislative e regolamentari vigenti e applicabili, con modalità automatiche, anche mediante sistemi informatizzati, solo ed esclusivamente nell'ambito delle operazioni necessarie a consentire l'accesso e l'utilizzazione delle Rete informatica e telematica dell'Università, e per finalità direttamente connesse e strumentali all'accesso e dell'utilizzazione della Rete stessa da parte del richiedente;
- di acconsentire con la presente dichiarazione, ai sensi dell'art. 23 del predetto D.lgs 196/2003 al trattamento dei propri dati personali, svolto con le modalità e per le finalità sopra indicate, ed in conformità alle norme legislative e regolamentari vigenti e applicabili;
- di essere a conoscenza del fatto di poter esercitare i diritti previsti dell'art. 7 del predetto D.lgs 196/2003, tra i quali il diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo/la riguardano, l'aggiornamento, la rettifica ovvero l'integrazione dei dati nonché la loro cancellazione, mediante comunicazione scritta da inoltrarsi allo stesso Referente informatico.

Milano, li _____

Firma: _____