FINAL 1.3

DOCUMENTO PUBBLICO

Acceptable Use Policy (AUP)

Parma, 13/06/2007

Introduzione

All'interno del presente documento sono descritte alcune norme comportamentali che gli utenti connessi ad Internet tramite l'infrastruttura di BT Enìa S.p.A. sono tenuti a rispettare.

La definizione di tali norme e di una metodologia di intervento in caso di abusi consente di perseguire i seguenti obiettivi:

- Preservare la reputazione e l'immagine di BT Enìa S.p.A. e dei propri clienti nei confronti della comunità Internet;
- Proteggere BT Enìa S.p.A., i propri clienti, e la comunità Internet da attività irresponsabili o illegali;
- Assicurare la privacy e l'affidabilità dei sistemi dei clienti BT Enìa S.p.A. ;
- Garantire l'affidabilità della rete e dei servizi erogati da BT Enìa S.p.A. .

1.1. Filtri

BT Enìa S.p.A. si riserva il diritto di creare in caso di necessità dei filtri sulle comunicazioni a livello rete o applicazione per evitare il manifestarsi di comportamenti non conformi alle norme comportamentali descritte nel presente documento.

BT Enìa S.p.A. si impegna ad applicare tali filtri in modo da non alterare il funzionamento dei servizi che non sono collegati all'attività illecita eventualmente segnalata e/o individuata.

Scopo di tali filtri è esclusivamente limitare qualsiasi tipo di attività non conforme alle norme comportamentali riportate nel presente documento. Al fine di perseguire tale obiettivo BT Enìa S.p.A. si riserva il diritto di oscurare l'eventuale autore di un abuso, previa notifica al Cliente.

1.2. Aspetti Legislativi

Si considera illecita qualsiasi attività punibile a norma di legge. In particolare, è proibito creare, trasmettere, pubblicare o archiviare qualsiasi tipo di materiale che:

- Infranga le leggi sul diritto d'autore e la proprietà intellettuale;
- Includa contenuti che siano dannosi, minatori, molesti, offensivi e/o calunniosi, diffamatori e/o calunniosi, volgari.
- Violi le leggi sulla Privacy;
- Violi le leggi sull'esportazione;
- Incoraggi il compiersi di azioni criminali.

1.3. Aspetti generali dell'abuso

Viene considerato "abuso" una qualsiasi violazione delle norme comportamentali descritte in questo documento nonché delle norme di buon uso delle risorse di

rete, contenute nel documento "Netiquette", e pubblicate sul sito web della Naming Authority Italiana (http://www.nic.it/NA/netiquette.txt). In particolare sono considerati “abusi” i seguenti comportamenti:

- Blocco o rallentamento di servizi erogati ad utenti autorizzati;
- Utilizzo di linguaggio offensivo o minaccioso;
- Spam;
- Azioni intrusive finalizzate alla raccolta di informazioni su reti e sistemi, utili per la pianificazione di un successivo attacco (detto ***probe***);
- Tentativi di intrusione;
- Alterazione dei dati relativi alla propria identità (detto ***spoofing***);
- Diffusione di virus o altro malicious software;

Sono considerati “abusi” anche tutte le situazioni in cui l’utente di BT Enìa S.p.A. non applica sufficienti meccanismi di protezione ai propri sistemi, offrendo punti di appoggio per attività contrarie al codice comportamentale descritto in questo documento. In particolare gli utenti della rete di BT Enìa S.p.A. sono tenuti a rispettare le seguenti direttive:

- Utilizzare e mantenere aggiornato il software Anti-Virus sui propri sistemi;
- Applicare dei meccanismi di controllo degli accessi sui Server Proxy e SMTP;

1.4. Posta Elettronica

Si considera quale trasmissione di Bulk E-mail qualsiasi processo di spedizione di messaggi di posta elettronica tramite meccanismi automatizzati.

La spedizione di Bulk E-mail deve essere espressamente autorizzata dai destinatari, in caso contrario tali messaggi saranno considerati unsolicited Bulk E-mail (tale attività è detta gergalmente *spam*).

Si considera abuso una qualsiasi attività contraria alla normativa vigente sul trattamento dei dati personali nell’utilizzo della posta elettronica quali ad esempio:

- Spedizione di messaggi di posta elettronica a fini pubblicitari, commerciali, politici, religiosi in assenza di una esplicita richiesta da parte dei destinatari;
- Spedizione di messaggi di posta elettronica dai contenuti osceni o offensivi nei confronti dei rispettivi destinatari;
- Spedizione di qualsiasi messaggio di posta elettronica verso destinatari che abbiano precedentemente richiesto il non invio degli stessi;

La sorgente di Bulk E-mail è tenuta a indicare sui messaggi di posta elettronica la modalità con la quale ha reperito l’indirizzo e-mail del destinatario e deve essere in grado di dimostrare ad BT Enìa S.p.A. l’effettiva presenza di una sottoscrizione precedentemente effettuata dagli stessi.

BT Enìa S.p.A. potrà utilizzare la tecnologia di filtraggio o altre misure atte a bloccare l'invio di messaggi di posta elettronica indesiderati.

1.5. Usenet

Si raccomanda di iniziare le operazioni di post all'interno di un newsgroup solo dopo aver familiarizzato con i suoi contenuti e dopo averne letto attentamente il manifesto.

L'utente è in ogni caso tenuto a rispettare le direttive contenute all'interno di tale manifesto.

In particolare sono vietate le seguenti attività:

- Effettuare operazioni di post a scopi commerciali o pubblicitari all'interno di newsgroup qualora non espressamente consentito dal relativo manifesto;
- Effettuare operazioni di post allegando file binari qualora non espressamente consentito dal relativo manifesto;
- Effettuare operazioni di cross-post in più di cinque newsgroup.

1.6. World Wide Web

Sono vietate le seguenti attività:

- Pubblicare materiale considerato osceno, offensivo, diffamatorio, minaccioso, violento o comunque reprensibile.
- Pubblicare software che violi le leggi sul diritto d'autore e sulla proprietà intellettuale;
- Pubblicare o diffondere materiale che favorisca attività illecite, quali ad esempio la pirateria informatica (hackers tools).

1.7. Dialers

Qualora attraverso un sito web venga proposta l'installazione di software di connessione verso numeri a tariffazione specifica (premium number dialers), devono essere applicate le seguenti direttive:

- In corrispondenza del link per il download del dialer deve apparire una chiara informativa che indichi la tariffa ed il numero chiamato;
- L'interfaccia grafica del dialer deve presentare le condizioni di servizio sulla prima schermata;
- Devono essere inclusi meccanismi in grado di verificare l'avvenuta lettura delle condizioni di servizio;
- La connessione deve essere permessa solamente dopo una formale accettazione delle condizioni di servizio;
- E' vietato l'utilizzo di meccanismi di spam per pubblicizzare il sito web in questione, a prescindere dai carrier di provenienza;
- IRC (Internet Relay Chat)

L'utilizzo dei servizi di chat deve essere conforme alle direttive indicate dal fornitore del servizio e in ogni caso non sono ammessi contenuti offensivi o osceni nei confronti degli interlocutori.

1.8. Attività di tipo "Hacking"

Sono considerate illecite tutte le attività volte a forzare abusivamente un qualunque sistema informatico.

In particolare sono proibite le seguenti attività:

- Effettuare operazioni non autorizzate di "probe" verso servizi non pubblicati all'interno della rete Internet. All'interno della comunità Internet si ritiene pubblico qualsiasi servizio indicizzato all'interno di database come il DNS ed i siti web;
- Effettuare qualsiasi tipo di attività volta a raggirare o compromettere i meccanismi di protezione dei sistemi informatici;
- Sfruttare qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinseci ai programmi e/o ai sistemi al fine di commettere azioni illecite o non autorizzate.
- Falsificare la propria identità (effettuare lo spoofing delle proprie credenziali, per esempio dell'indirizzo IP o dell'indirizzo e-mail);
- Falsificare (detto gergalmente ***forgiare***) il contenuto degli header dei protocolli di comunicazione;
- Trasmettere software che alteri il normale funzionamento del sistema informatico del destinatario (virus, worm o altro malicious software);
- Impedire ad altri utenti di utilizzare un servizio tramite attacchi di tipo DoS (Denial of Service).

1.9. La funzione di Abuse Desk

Le segnalazioni relative ad eventuali abusi (ossia attività non conformi alle direttive contenute all'interno del presente documento) devono essere recapitate all'Abuse Desk tramite l'indirizzo di posta elettronica abuse.italy.g@bt.com

In caso di bisogno l'Abuse Desk può utilizzare ulteriori mezzi per la raccolta di tali segnalazioni (per esempio un form via web).

L'Abuse Desk non può fornire informazioni personali riguardanti i propri clienti. Qualora gli stessi siano ritenuti fonte di abusi l'Abuse Desk si riserva il diritto di compiere le necessarie analisi ed indagini affinché si impedisca il ripetersi di tali abusi.