F I D O N E T

Guida Operativa e Procedurale

Regione 33 / Italia

Novembre 1990

Introduzione

Questo documento integra il regolamento generale FidoNet in vigote (Policy) per la Regione 33 / Italia.

1 National Mail Hour.

La Regional Mail Hour della Regione 33 ha una durata di 60 minuti e coincide con la Zone Mail Hour della Zona 2 cosi' come definita dal coordinatore di Zona.
Tutti gli orari sono GMT (tempo medio di Greenwich), equivalenti all'ora solare italiana meno 1 ora o alla ora legale italiana meno due ore.
I sysop che aggiornano l'orario del calcolatore sull'ora legale, quindi, sono tenuti ad adattare gli orari degli eventi di conseguenza.
Durante il periodo della ZMH tutti i nodi FidoNet debbono sospendere l'accesso agli utenti ed accettare solo collegamenti con altri nodi della rete, rifiutando eventuali file-request.
I coordinatori di Net possono definire periodi aggiuntivi mail-only per risolvere problemi di trasferimento dati all'interno del net.

2 Crash-Mail.

L'uso della crash-mail (ovvero l'inoltro immediato dei messaggi senza il rispetto degli orari stabiliti al punto 1) e' consentito solo se assume carattere di saltuarieta'.
L'uso della crash-mail su base sistematica e' considerato comportamento scorretto, e puo' comportare le sansioni previste nel documento di policy generale.
Comportamente scorretto e' considerato anche l'inoltro di messaggi in Crash a nodi che non hanno il relativo flag (CM) nella nodelist.

3 Nodelist.

I coordinatori di ogni livello devono inviare la nodelist al coordinatore del livello immediatamente superiore entro la fine della regional mail hour del martedi', in modo che possa essere inclusa nella lista ufficiale dei nodi italiani, che viene generata ogni mercoledi'.

4 Point.

Ogni nodo puo' costituire una sua sotto-rete. In questo caso il nodo ufficiale viene definito 'Boss', mentre i singoli componenti della sotto-rete 'Point'.
Il nodo che desidera creare una sua sotto-rete deve utilizzare un

numero di net fittizio (fake-net) che deve essere assegnato dal coordinatore di net.
Il numero fake-net sara' assegnato utilizzando un codice parlante costituito di cinque cifre costituito in questo modo: la prima cifra e' fissa a 2, la seconda e' costituita dall'ultima cifra del numero di net, le rimanenti tre sono il numero del nodo del boss. Ad esempio: il point 10 del nodo 2:331/301 verra' identificato con l'indirizzo 2:21301/10.

Questo sistema di indirizzamento e' comunemente detto "point 3D", perche' il point viene identificato con un numero a tre dimensioni (zona, net e nodo).

I point in grado di operare, tramite apposito software, senza usare una fake-net e che quindi sono in grado di effettuare sessioni facendosi identificare con un indirizzo a quattro dimensioni (completo cioe' di zona, net, nodo e numero di point) vengono comunemente detti "point 4D".

Ogni Point comunica con la rete FidoNet solo ed esclusivamente attraverso il suo Boss; non e' quindi ammesso l'uso della Crash-Mail (ne' di altri collegamenti diretti) ai point 3D, ovvero ai point che fanno uso di fakenet.
E' concesso eccezionalmente ai soli point 4D l'uso della Crash-Mail per inviare direttamente messaggi a nodi diversi dal proprio boss, fermi restando il rispetto degli orari e degli standard tecnici della rete e l'utilizzo di una nodelist (REGION.033) aggiornata.

5 File-Request.

Ogni nodo e' libero di gestire autonomamente la disponibilita' al file-request. E' quindi buona norma entrare in contatto preventivo per richiedere una eventuale autorizzazione.
E' fatto comunque invito ai nodi della rete di mettere a disposizione di tutti un file richiedibile con il magic filename ABOUT, contenente indicazione delle modalita' (ed eventuali restrizioni) di accesso al file-request; tale messaggio costituirebbe autorizzazione implicita a ogni file-request che rispetti tali norme.
I point possono effettuare file-request con le medesime modalita'.

6 Comportamenti scorretti.

E' espressamente vietato utilizzare la rete FidoNet per insultare altre persone, nazioni, razze, lingue o religioni.
E' altresi' categoricamente vietato inviare messaggi contenenti informazioni illegali come codici e metodi per accedere a sistemi di elaborazione dati privati, o pubblici a pagamento.

Ogni Sysop puo' decidere autonomamente la gestione del proprio nodo, ma e' indispensabile che osservi gli eventi mail stabiliti, non arrechi disturbo ad altri nodi della rete, e non promuova la distribuzione illegale di software coperto da copyright.
E' quindi espressamente e categoricamente vietato mettere a disposizione degli utenti, di qualsiasi livello, software protetto da diritto d'autore che non abbia specifica autorizzazione alla distribuzione via BBS o mezzi equivalenti.

8 Conferenze Sysop.

Ogni sysop della regione 33 dovrebbe essere connesso con la conferenza SYSOP.033, che costituisce il veicolo di informazione della rete stessa. Tutte le notizie riguardanti la rete, infatti, vengono distribuite solo ed esclusivamente attraverso questo canale. Tutti i coordinatori, invece, devono essere connessi alla conferenza COORD.033.

9 Compatibilita' con altre reti.

E' garantita a ogni sysop Fidonet la facolta' di aderire contemporaneamente a piu' reti, purche' le sue attivita' e comportamenti entro dette reti siano conformi agli ideali di legalita' perseguiti da Fidonet. Ove si avesse prova che un sysop Fidonet, pur corretto e in regola con le policy Fidonet nell'ambito delle sue attivita' Fidonet, abbia tenuto in altre reti comportamenti illegali (con particolare riferimento allo scambio di password, ad azioni e metodi di hacking ed allo scambio o commercio di software piratato), sara' facolta' del Coordinatore competente sanzionarlo secondo quanto previsto dalle policy Fidonet.

E' dichiarata decaduta qualsiasi eventuale limitazione esistente (a livello locale o di region) relativa all'ammissione di nuovi membri in Fidonet e basata solo sulla loro appartenenza ad altre reti, a patto che il loro comportamento sia e resti conforme alle linee di condotta sopra delineate.

10 Messaggi crittografati.

E' vietato l'instradamento di messaggi crittografati attraverso i Coordinatori di Net, in quanto la crittografazione rende impossibile la verifica del contenuto dei messaggi in transito allo scopo di accertarsi che la rete non venga utilizzata per fini illegali o commerciali.

I messaggi crittografati inoltrati ai Coordinatori di Net devono essere respinti al mittente seguendo la procedura descritta al punto 2.1.7 della Policy Fidonet (Policy4I). L'instradamento di messaggi crittografati attraverso la normale route netmail costituisce comportamento seccante.

11 Sovraccarico netmail.

Quantita' eccessive di messaggi da parte di un singolo nodo possono degradare la capacita' della rete FidoNet di gestire il normale traffico di posta e costituiscono percio' comportamento seccante.

Rientrano in questa categoria i messaggi generati automaticamente da programmi-robot (es. ALLFIX, Ghostwriter, etc.), i messaggi inviati in copia ad un numero elevato di destinatari (bombing run), i file uuencodati di lunghezza superiore agli 8Kb, etc.

Se un nodo del Net genera sovraccarico netmail, il Coordinatore puo' chiedere al suo Sysop di limitarne la quantita', o di terminarne l'instradamento.

12 Altro.

Per quanto non espressamente previsto si rimanda alla regolamentazione della zona 2 (PolicyZ2) e della organizzazione mondiale fidonet (policy4I).