Serviciul Cazare Studenți

ACADEMIA DE STUDII ECONOMICE DIN BUCUREŞTI
Serviciul Cazare Studenţi
Str. Frumoasă, nr. 31, camera 13, sector 1, Bucureşti
Site: www.cazare.ase.ro E-mail: serviciulcazare@ase.ro

DECLARAŢIE PE PROPRIE RASPUNDERE

Prin prezenta, subsemnatul/a ....., student/ă la Facultatea..... din cadrul Academiei de Studii Economice din Bucureşti, anul ....., forma ....., în calitate de locatar al caminului ....., camera ....., declar pe proprie răspundere că am luat la cunoștință sarcinile care îmi vor reveni odată cu alegerea mea ca responsabil de rețea, că sunt DE ACORD cu acestea și că mă voi ocupa de îndeplinirea lor.

Data.....

LOCATAR,
Student/ă
.....

Definire termeni:

Zonă	Unitatea administrativă de organizare a studenţilor, în vederea gestionării serviciului de acces la reţeaua A.S.E şi Internet. Din punct de vedere administrativ, *zona* reprezintă unitate indivizibilă pentru Direcția T.I.C.
Reprezentant	Persoana desemnată de studenţii unei zone (după criteriile şi în modalitatea dorită de aceştia) pentru a-i reprezenta în relaţia cu Direcția T.I.C. Dacă studenţii doresc acest lucru, poate fi acelaşi Reprezentant pentru mai multe zone. O zonă poate avea mai mulţi reprezentanţi.
Cablare structurată	Infrastructură a reţelei de date, realizată atât pe plan orizontal cât şi pe plan vertical în cadrul unei clădiri. Exemplu: prizele de date din fiecare cameră sunt conectate la switch prin intermediul traseelor de cablu şi a patch panel-urilor, acestea fiind amplasate pe fiecare nivel (etaj) al clădirii într-un rack de conexiuni (infrastructură pe orizontală). Echipamentele active ce se găsesc montate pe fiecare nivel, se conectează prin intermediul traseelor de cablu şi a patch panel-urilor la un echipament de backbone (infrastructură pe verticală).
Atacuri informatice	Acţiuni prin care sunt afectate reţelele de calculatoare ale unei organizaţii cu scopul de a sabota activitatea sau de a obţine informaţii secrete.

1. Responsabilităţile Reprezentantului şi penalităţi:
   1) **Reprezentantul** va lua toate măsurile pentru a asigura protecţia computerelor faţă de viruşi informatici şi alte programe de acest gen. În momentul în care vor apărea sisteme infectate sau vulnerabile la infecţii cunoscute, zona respectivă va fi deconectată, pentru cel puţin **3 zile** până la eliminarea infecţiilor sau vulnerabilităţilor. Pentru soluţionarea acestor probleme, Directia T.I.C. pune la dispoziţia Reprezentantului atât un CD cu update-uri, patch-uri pentru sistemul de operare, antivirus, cât şi un sistem special de acces la reţea doar către un server de fişiere, de unde se pot descărca cele menţionate mai sus.
   2) În cazul în care există cablare structurată în zona respectivă, Reprezentantul nu are voie să intervină asupra prizelor de date! De asemenea, Reprezentantul se angajează să ţină o evidenţă a prizelor de date cu probleme din zona respectivă şi periodic să aducă la cunoştiinţa Direcția T.I.C., situaţia la zi a acestor echipamente.
   3) Reprezentantul va încerca să păstreze o stare de înţelegere faţă de accesul la reţea în cadrul zonei pe care o reprezintă. Dacă vor apărea neînţelegeri/discuţii care vor escalada până la Direcția T.I.C., întreaga zonă va fi deconectată pentru **3 zile**.
   4) În cazul atacurilor iniţiate din cadrul unei *zone* către restul reţelei A.S.E. sau către Internet, *zona* va fi deconectată pentru **1 săptămână**.
   5) Orice intervenţie asupra dulapurilor cu echipamente active de reţea instalate în cămin se va face numai de către Direcția T.I.C. În cazul accesului neautorizat la un dulap, *zona* deservită de acesta va fi deconectată pentru **1 săptămână**.
   6) Adresele IP în cadrul reţelei din Cămin vor fi gestionate prin serviciul DHCP administrat de către Direcția T.I.C. În afara cazurilor speciale în care se va cere acest lucru de către Direcția T.I.C., studenţii **NU** îşi vor configura echipamentele cu adrese IP statice. Echipamentele care vor fi configurate cu adrese IP statice vor fi izolate de

restul reţelei A.S.E. pentru **1 săptămână**. Acesta este singurul caz în care deconectarea se va face la nivel de staţie şi nu la nivel de *zonă*.

7) În condiţiile în care se va schimba Reprezentantul unei zone, schimbarea va fi comunicată imediat Direcției T.I.C., împreună cu datele de contact pentru noul Reprezentant, iar noul Reprezentant se va prezenta pentru semnarea acestui document în termen de maxim 1 săptămână. În caz contrar, zona respectivă va fi deconectată până la îndeplinirea acestei condiţii. O zonă care nu are Reprezentant NU va fi conectată la reţeaua A.S.E.
8) Reprezentantul va informa Direcția T.I.C. în legătură cu orice schimbare în datele sale de contact.
9) Reprezentantul are obligaţia de a menţine şi pune la dispoziţia Direcția T.I.C. o bază de date cu toate echipamentele conectate la reţeaua din zona sa. Datele care vor fi cuprinse în această bază de date, precum şi modalitatea de transmitere a acesteia către Direcția T.I.C. vor fi stabilite ulterior. Orice schimbare (adăugarea unui nou computer, schimbarea plăcii de reţea, etc.) va fi comunicată în timp util Direcția T.I.C. de către Reprezentant.
10) Orice sesizare catre Direcției T.I.C., legata de imposibilitatea de conectare la retea a unei statii de lucru din zona responsabila, va fi insotita de urmatoarele informatii: numarul camerei, caminul, adresa MAC a placii de retea, adresa IP a statiei, rezultatul testului de conectare directa la priza de retea a statiei (in cazul in care in camera respectiva exista un switch sau router).

2. Alte prevederi:
   1. **Direcția T.I.C.** va încerca să informeze **Reprezentanţii** în legătură cu toate vulnerabilităţile şi infecţiile curente, şi va oferi utilitare şi informaţii pentru protejarea împotriva acestora prin intermediul paginii web a Direcția T.I.C., www.net.ase.ro . Este însă responsabilitatea Reprezentanţilor de a asigura protecţia sistemelor din cadrul zonei.
   2. **Direcția T.I.C.** va răspunde tuturor sesizărilor venite pe adresa it-suport@ase.ro sau a sesizărilor făcute la secţiunea *CONTACT* de pe pagina www.net.ase.ro.
   3. **Reprezentantul** se va asigura ca echipamentele studentilor de tip ROUTER, din zona administrată, sunt configurate corect. În cazul în care **Reprezentantul** nu poate configura echipamentul se va prezenta cu el la **Direcția T.I.C.** pentru configurare.
   4. **Reprezentanții** trebuie să acceseze, în mod regulat, platforma http://172.30.5.15/, platformă pe care se vor conecta cu ajutorul conturilor individuale, distribuite de către Direcția T.I.C. la semnarea unui "Protocol de conectare". **Reprezentanții** au obligația de a completa o fișă de incident pentru fiecare intervenție realizată. Incidentele se vor adăuga/modifica pe pagina INCIDENT TRACKING. De pe pagina TOOLS se pot descărca script-uri, care pot fi folosite de către reprezentant pe orice sistem, în vederea aplicării setărilor de rețea corespunzătoare.

   5. Script-urile conțin următoarele funcții:

      - setare adresa IP automat (DHCP pornit)
      - Flush DNS
      - Setare server proxy automat (proxystudent.ase.ro)Înţeleg şi sunt de acord să respect cele scrise mai sus