

SZKOLENIE TECHNICZNE
Bezpieczne korzystanie z komputera, prawa autorskie oraz ochrona własności intelektualnej

Propozycja szkolenia przeznaczona jest dla wszystkich użytkowników końcowych systemów komputerowych, którzy chcą w bezpieczny sposób korzystać z komputera i zasobów Internetu. Na szkoleniu omawiane są wszelkie zagrożenia wynikające z niewiedzy użytkownika, począwszy od zagrożeń w sieci po zagrożenia wynikające z niezastosowania polityki bezpieczeństwa w firmie lub też niestosowania jej przez pracowników na co dzień.

Każdy uczestnik, który zakończy szkolenie egzaminem otrzyma Certyfikat Autoryzowanego Centrum Szkoleniowego DAGMA.

Czas: 6h (10:00-16:00)

Harmonogram szkolenia:

1. Zasady bezpiecznego korzystania z komputera.

2. Zagrożenia bezpieczeństwa teleinformatycznego w instytucjach administracji publicznej.

3. Bezpieczeństwo w zakresie użytkownika końcowego

- a) wykorzystanie sprzętu komputerowego,
- b) polityka haseł,
- c) blokowanie komputera – eliminacja nieautoryzowanego dostępu do stacji roboczej,
- d) dodatkowa ochrona- wygaszacze ekranu z hasłem, hasła w systemach Bios,
- e) bezpieczeństwo fizyczne danych przetwarzanych, składowanych,
- f) szyfrowanie danych przetwarzanych jak i składowanych jako ochrona przed nieautoryzowanym dostępem,
- g) szyfrowanie transmisji danych zawierających treści poufne,
- h) zasady bezpiecznego wykorzystania zasobów Internetu, korzystanie z serwisów,
- i) www, komunikatorów, zasobów sieciowych,

4. Ustawa o ochronie danych osobowych, [ustawa ODO 1997].

- a) założenia zastosowanie

5. Pozostałe akty prawne w odniesieniu do bezpieczeństwa teleinformatycznego.

- b) Ustawa o *rachunkowości* [1994]
- c) Ustawa o *ochronie informacji niejawnych* [ustawa OIN 1999]
- d) Ustawa o *prawie autorskim i prawach pokrewnych* [ustawa PAiPP 1994]
- e) Ustawa o *systemie ubezpieczeń społecznych* [ustawa SUS 1998]
- f) Ustawa o *podpisie elektronicznym* [ustawa PE 2001]
- g) Ustawa *Kodeks Karny* [k.k. 1997]

6. Zagrożenia w sieci.

- a) zagrożenia socjotechniczne,
- b) udostępnianie zasobów osobom nieuprawnionym,
- c) pobieranie nielegalnego oprogramowania, plików chronionych prawem autorskim,
- d) wirusy, trojany, rootkit, oprogramowanie spyware,
- e) sposoby wykrywania, eliminacji, redukcji zagrożeń,

7. Dobre praktyki bezpiecznego używania komputerów w instytucjach administracji publicznej.

8. Własność intelektualna, prawa autorskie, piractwo.

- a) podstawowe definicje,
- b) własność intelektualna w aspekcie praw autorskich,
- c) rodzaje piractwa komputerowego,
- d) piractwo komputerowe, metody przeciwdziałania, zwalczania, zarys możliwości technicznych oraz prawnych,
- e) regulacje prawne odnoszące się do praw autorskich, konsekwencje, zakres odpowiedzialności, odpowiedzialność cywilna oraz karna.

9. Instytucje chroniące prawa autorskiego w Polsce, zakres działalności, kompetencje.

10. Zasady właściwego wykorzystania oprogramowania.

- a) EULA – definicja, określenie warunków korzystania z oprogramowania,
- b) dokumenty zarządzania oprogramowaniem, prawne możliwości ochrony własności,
- c) intelektualnej w urzędach publicznych,
- d) zasady przechowywania atrybutów legalności oprogramowania,
- e) zasady instalowania, usuwania oprogramowania,
- f) efektywne zarządzanie oprogramowaniem,
- g) dobre praktyki,

11. Egzamin (opcjonalnie).