e-Guardian Version 1.0 Syllabus		
Kategoria	Ref.	Zadanie
1. Podstawowe środki zapewniania bezpieczeństwa	1.1	Posiadanie wiedzy o tym jak śledzić zmiany wersji oprogramowania, jak zaopatrywać się w uaktualnienia i stosować je wraz z dodatkowym oprogramowaniem i komponentami bezpieczeństwa w użytkowanym systemie operacyjnym. Rozumienie korzyści wynikających z aktualizacji.
	1.2	Znajomość systemu kont użytkowników. Rozumienie czym jest osobiste konto użytkownika i jak odseparować dane poszczególnych użytkowników.
	1.3	Rozumienie celu stosowania nazwy użytkownika oraz różnicy między nazwą a hasłem użytkownika. Rozumienie znaczenia i wagi praw dostępu.
	1.4	Rozumienie konieczności logowania do systemu hasłem. Użycie haseł logowania.
	1.5	Umiejętność tworzenia haseł złożonych. Znajomość budowy haseł złożonych oraz zasady zmian i trwałość haseł.
	1.6	Umiejętność włączenia/wyłączenia oraz poprawiania poziomu ochrony w standardowych środkach bezpieczeństwa zawartych w systemie operacyjnym (Firewall , Defender).
	1.7	Posiadanie wiedzy o ochronie danych na dysku komputera, rozumienie pojęcia szyfrowania danych i ochrony hasłem.
	1.8	Umiejętność rozróżnienia czy nośnik danych ma możliwość ochrony hasłem przed nieupoważnionym dostępem (do danych). Stosowanie takiego hasła. Umiejętność ochrony nośników CD, DVD, pamięci USB oraz innych zewnętrznych nośników danych.
	1.9	Rozumienie zagrożeń rozprzestrzenianych przez złośliwe oprogramowanie na zewnętrznych nośnikach danych.
	1.10	Rozumienie celu i korzyści wynikających ze stosowania kopii zapasowych (backup) danych i oprogramowania.
	1.11	Posiadanie wiedzy o tym, kogo należy zawiadomić po wykryciu albo podejrzeniu, że dane, pliki itp. mogą być sklasyfikowane jako nielegalne albo niebezpieczne.
2.Złośliwe oprogramowania	2.1	Rozumienie, rozpoznawanie, definiowanie różnego rodzaju złośliwego oprogramowania (wirusy, konie trojańskie, oprogramowania szpiegowskie)
	2.2	Określanie jak i kiedy złośliwe oprogramowanie może dostać się do systemu operacyjnego komputera.
	2.3	Stosowanie różnego rodzaju oprogramowania jako ochrony przed złośliwym oprogramowaniem.
	2.4	Konfigurowanie oprogramowania (antywirusowego) do regularnych i automatycznych uaktualnień.
	2.5	Posiadanie wiedzy na temat procedur postępowania, w przypadku gdy komputer zostanie zainfekowany złośliwym oprogramowaniem. Rozumienie ograniczeń oprogramowania zabezpieczającego.
	2.6	Rozumienie, że podczas kopiowania plików z Internetu oraz odbierania załączników w wiadomościach e-mail musi być uruchomiona aktualna wersja oprogramowania zabezpieczającego.
	2.7	Rozumienie faktu, że niechciane i nieznane wiadomości e-mail nie powinny być otwierane.
	2.8	Rozumienie czym jest niebezpieczny nośnik danych. Rozumienie faktu, że niepewne nośniki danych CD, DVD pamięci USB nie powinny być używane.
3.Wiadomości elektroniczne	3.1	Posiadanie wiedzy o wiadomościach e-mail sklasyfikowanych jako spam oraz o wiadomościach zawierających złośliwe oprogramowanie.
	3.2	Posiadanie wiedzy o ustawodawstwie dotyczącym ochrony prywatności.
	3.3	Umiejętność przekierowania wiadomości e-mail z konta dziecka na konto rodzica.
	3.4	Umiejętność odrzucania wiadomości e-mail przychodzących z konkretnych adresów.
	3.5	Umiejętność blokowania wymiany prywatnych wiadomości między dzieckiem a inny użytkownikiem.
	3.6	Posiadanie wiedzy na temat procedur obchodzenia się z wiadomościami e-mail od nieznajomych nadawców.
	3.7	Rozumienie poziomu zabezpieczeń komunikatorów (instant messaging).

	3.8	Rozumienie możliwości telefonów komórkowych w zakresie przekazywania informacji.
	3.9	Posiadanie wiedzy o tym, z kim się skontaktować w przypadku wykrycia lub podejrzenia że zawartość jest nielegalna lub niebezpieczna.
4.Bezpieczne przeglądanie zasobów www i dokonywanie płatności w Internecie	4.1	Umiejętność stosowania narzędzi zapewniających bezpieczeństwo podczas przeglądania zasobów WWW (blokowanie ciasteczek, kontrola technologii ActiveX – wyskakujących okienek).
	4.2	Rozumienie wad, zalet oraz niebezpieczeństw związanych z ciasteczkami.
	4.3	Wiedza o niebezpieczeństwie związanym z ujawnianiem danych osobowych.
	4.4	Rozumienie zagrożeń i luk bezpieczeństwa w użyciu sieci Internet, takich jak wykorzystanie lub kradzież tożsamości lub informacji o osobie.
	4.5	Stosowanie kluczy szyfrowania w komunikacji w Internecie, rozróżnianie rodzajów kluczy szyfrowania i sposoby ich użycia.
	4.6	Umiejętność rozróżniania bezpiecznej/prawdziwej strony internetowej do transakcji od strony niebezpiecznej/fałszywej.
	4.7	Umiejętność przeprowadzania transakcji internetowej przy użyciu karty.
	4.8	Umiejętność skontaktowania się z administratorem serwisu, gdy jest to konieczne.
	4.9	Posiadanie wiedzy o tym, z kim się skontaktować w przypadku wykrycia lub podejrzenia nielegalnej lub niebezpiecznej zawartości.
5. Bezpieczeństwo dzieci	5.1	Rozumienie roli otwartej relacji między rodzicami a dzieckiem jako ważnego czynnika do zapewnienia dziecku bezpieczeństwa w cyberprzestrzeni.
	5.2	Rozumienie zagrożenia internetowych oszustw finansowych, złośliwego oprogramowania, cyberdręczenia, perwersyjności i pornografii w Internecie.
	5.3	Rozróżnianie rodzajów systemów monitorowania i umiejętność monitorowania używania komputera.
	5.4	Umiejętność przeglądania internetowych plików tymczasowych i historii przeglądarki.
	5.5	Stosowanie oprogramowania do kontroli użycia przez dzieci Internetu, systemu operacyjnego i oprogramowania użytkowego
	5.6	Stosowanie oprogramowania chroniącego dzieci.
	5.7	Umiejętność użycia zintegrowanych z przeglądarką internetową narzędzi filtrujących zawartość witryn.
	5.8	Stosowanie oprogramowania zabezpieczającego.
	5.9	Rozróżnianie wartości i stosowanie oprogramowania typu anty-wirus, anty-spam, anty-spyware i firewall.
	5.10	Umiejętność uzyskania dostępu do historii komunikacji chat i historii komunikatorów internetowych.
	5.11	Umiejętność skontaktowania się z administratorem serwera.
	5.12	Posiadanie wiedzy na temat stron internetowych rekomendowanych dla dzieci oraz wyszukiwarek nastawionych na dzieci i nastolatków.
	5.13	Posiadanie wiedzy o tym, z kim się skontaktować w przypadku wykrycia niebezpiecznych lub nielegalnych zawartości.