MANOWIECKI
CYBERSECURITY LAW

Procedura
reakcji w przypadku wystąpienia incydentu

1. Kiedy powinieneś zgłosić incydent?

Natychmiast zgłoś sprawę do działu IT, jeśli zauważysz którąkolwiek z poniższych sytuacji:

- Kliknąłeś/ęłaś w link lub pobrałeś/aś załącznik z wiadomości, która (po fakcie) wydaje Ci się dziwna (np. fałszywa faktura, rzekoma wiadomość od kuriera lub szefa).
- Na Twoim monitorze pojawił się komunikat o zaszyfrowaniu plików z żądaniem zapłaty.
- Kursor myszy porusza się sam, aplikacje otwierają się bez Twojej ingerencji, kamera internetowa włączyła się samoczynnie.
- Nie możesz otworzyć swoich dokumentów, a ich nazwy lub rozszerzenia zmieniły się na ciąg niezrozumiałych znaków (np. plik.docx.encrypted).
- Straciłeś/aś służbowy laptop, telefon, tablet lub pendrive.
- Przypadkowo wysłałeś plik z danymi osobowymi lub poufnymi danymi firmy do niewłaściwego adresata.

2. Jak reagować?

Jeżeli podejrzewasz, że Twój komputer został zainfekowany, wykonaj dokładnie te 3 kroki:

- Natychmiast odłącz komputer od sieci:
  - Wyciągnij kabel sieciowy (Internetowy) z komputera.
  - Jeśli korzystasz z Wi-Fi, użyj przełącznika/skrótu klawiszowego, aby wyłączyć sieć bezprzewodową lub włącz "Tryb Samolotowy".
  Powyższe pozwoli na odcięcie złośliwego oprogramowania od reszty firmy i serwerów.

- Odejdź od komputera i zrób notatki:
  - Zapisz na kartce godzinę zdarzenia i to, co dokładnie zrobiłeś przed awarią (np. "O 08:20 otworzyłem załącznik faktura.pdf z maila od J. Kowalskiego").
  - Zrób zdjęcie ekranu telefonem, jeśli wyświetla się na nim ważny komunikat.

- Powiadom IT (Telefonicznie):
  - Zadzwoń do działu IT. Nie pisz e-maila! Jeśli padłeś ofiarą ataku, przestępcy mogą czytać Twoją korespondencję lub system pocztowy firmy może być już niedostępny.

Adresat procedury: **Użytkownicy**

3. Czego BEZWZGLĘDNIE nie robić?

Z punktu widzenia bezpieczeństwa firmy, poniższe działania są surowo zabronione:

- NIE wyłączaj zasilania i nie restartuj komputera! Wyłączenie prądu czy resetowanie systemu bezpowrotnie niszczy cenne dowody zapisane w pamięci RAM, które są niezbędne dla informatyków śledczych. Pozostaw komputer włączony (tylko odłączony od sieci).
- NIE próbuj naprawiać problemu samodzielnie. Nie uruchamiaj skanerów antywirusowych na własną rękę, nie usuwaj dziwnych plików, nie próbuj "cofać" zmian.
- NIE przesyłaj podejrzanych e-maili dalej. Jeżeli chcesz pokazać koledze podejrzaną wiadomość, nie przesyłaj jej (przekaż dalej). Zadzwoń do niego i ostrzeż go słownie.
- NIE ukrywaj incydentu. Zamiatanie problemu pod dywan to najgorsze, co możesz zrobić. Wczesne przyznanie się do błędu (np. wpisania hasła na fałszywej stronie) pozwala IT zmienić hasło, zanim przestępca z niego skorzysta.

4. Ważne kontakty

Kogo powiadomić?	W jakiej sytuacji?	Kontakt?
Dział IT	Podejrzane e-maile, wirusy, dziwne zachowanie komputera.	adres e-mail: … nr tel.: …
Bezpośredni przełożony	Zgubienie sprzętu, wyciek danych poza firmę.	adres e-mail: … nr tel.: …
Pełnomocnik ds. SZBI	Potrzeba dodatkowych konsultacji w przypadku wystąpienia incydentu.	adres e-mail: … nr tel.: …
IOD (jeśli wyznaczono)	Wysłanie e-maila z danymi osobowymi do złej osoby.	adres e-mail: … nr tel.: …