На основу члана 11. став 4. Закона о информационој безбедности („Службени гласник РС”, број 6/16) и члана 42. став 1. Закона о Влади („Службени гласник РС”, бр. 55/05, 71/05 – исправка, 101/07, 65/08, 16/11, 68/12 – УС, 72/12, 7/14 – УС и 44/14),

Влада доноси

# УРЕДБУ
# О ПОСТУПКУ ДОСТАВЉАЊА ПОДАТАКА, ЛИСТИ, ВРСТАМА И ЗНАЧАЈУ ИНЦИДЕНАТА И ПОСТУПКУ ОБАВЕШТАВАЊА О ИНЦИДЕНТИМА У ИНФОРМАЦИОНО-КОМУНИКАЦИОНИМ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА

## Предмет уредбе

Члан 1.

Овом уредбом уређује се поступак достављања података о инцидентима у информационо-комуникационим системима од посебног значаја (у даљем тексу: ИКТ системи од посебног значаја) који могу да имају значајан утицај на нарушавање информационе безбедности, листа, врсте и значај инцидената и поступак обавештавања о инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности.

## Листа и значај инцидената

Члан 2.

Оператор ИКТ система од посебног значаја дужан је да пријави следеће инциденте:

1) инциденти који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга;

2) инциденти који утичу на велики број корисника услуга;

3) инциденти који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружања услуга, који утичу на обављање послова и вршење услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност;

4) инциденти који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;

5) инциденти који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе.

Оператор ИКТ система од посебног значаја дужан је да пријави и инциденте који су довели до значајног повећања ризика од наступања последица из става 1. овог члана.

**Врсте инцидената**

Члан 3.

Приликом пријаве инцидента оператор ИКТ система од посебног значаја одређује врсту инцидента, која може бити:

1) провољивање у ИКТ систем – напад на рачунарску мрежу и серверску инфраструктуру у оквиру кога је, кршењем мера заштите, остварен приступ који омогућава неовлашћен утицај на рад ИКТ система;

2) отицање података – доступност заштићених података ван круга лица овлашћених за приступ подацима;

3) неовлашћена измена података;

4) губитак података;

5) прекид у функционисању система или дела система;

6) ограничавање доступности услуге (енгл. denial of service attack);

7) инсталирање злонамерног софтвера у оквиру ИКТ система;

8) неовлашћено прикупљање података путем неовлашћеног надзора над комуникацијом или социјалним инжењерингом;

9) непрестани напад на одређене ресурсе;

10) злоупотреба овлашћења приступа ресурсима ИКТ система;

11) остали инциденти.

Поједини инцидент може бити разврстан у више врста инцидената из става 1. овог члана.

**Поступак обавештавања**

Члан 4.

Оператор ИКТ система од посебног значаја обавештење о инциденту доставља министарству надлежном за информациону безбедност (у даљем тексту: Надлежни орган), Народној банци Србије односно регулаторном телу за електронске комуникације писаним путем без одлагања, најкасније наредног радног дана од дана сазнања о настанку инцидента, а оператори ИКТ система за рад са тајним подацима поступају у складу са прописима којима се уређује област заштите тајних података.

Обавештење о инциденту мора да садржи врсту и опис инцидента, време и трајање инцидента, последице које је инцидент изазвао, предузете активности ради ублажавања последица инцидента и, по потреби, друге релевантне информације.

У случају хитности информација о инциденту се додатно пријављује телефонским путем, путем електронске поште или на други одговарајући начин.

Надлежни орган, Народна банка Србије и регулаторно тело за електронске комуникације могу ближе уредити поступак обавештавања о инцидентима, у складу са овом уредбом.

**Завршна одредба**

Члан 5.

Ова уредба ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.