# INSTRUCTION
# THE PROCEDURE FOR USERS TO RESPOND TO INFORMATION SECURITY INCIDENTS AND IN EMERGENCY (CRISIS) SITUATIONS

**Astana**
**2023**

## Terms and abbreviations

Organization - Qazaq Green Association of RES;

**Instruction** - Instruction on the procedure for user response to information security incidents and in extraordinary (crisis) situations of the Organization.

**Password compromise** - the leaking or disclosure of a password.

**Unauthorized access to information** (hereinafter referred to as "UAI") - access to information that violates the rules of access differentiation using standard means provided by computer hardware or automated systems.

**The first supervisor** shall be the Director or a person acting in his/her capacity;

**Provider - a** legal entity (entities) providing services on placement of equipment of specialized information systems, connection to the Internet and other services related to the maintenance of the systems.

**Information Security Specialist (hereinafter - IS)** - an Employee of the Organization who provides support and development of the Organization's IT infrastructure.

**Threat** - The potential cause of an unwanted incident that could cause damage to the system or the Organization.

**SW** - software.

**LAN** - local area network of the Organization.

**System Administrator** (hereinafter - SA) - an employee who performs the functions of administration of servers and application active equipment of the corporate information network, in accordance with the Organization's System Administrator Job Description.

## 1. General Provisions

1. This Instruction defines the procedure for actions of users of the corporate computer network, system administrator, information security specialist and administrative services of office operation in case of emergency (crisis) situations in the Organization.

2. This Instruction treats as an out-of-state situation:

1) prolonged lack of communication with the server;
2) software failure resulting in inability to further process information;
3) password compromise;
4) server or network equipment failure;
5) loss or leakage of information on a server or personal computer;
6) an attempt of intrusion detected by the means of registration;
7) Intrusion into the IS or detection of malicious code in software;
8) failure of communication channels;
9) power failure resulting in complete or partial loss of IS operability,

inability to process information by the Organization's computing equipment;

10) natural climatic impacts (earthquake, floods, hurricanes, fires, etc.);

11) other impact on information resources resulting in partial loss of IS operability (failure of individual system components, loss of performance, violation of integrity and confidentiality of programs and information) or complete IS failure (inability to further perform its functions, destruction, blocking, unlawful modification or compromise of information).

3. Sources of information about the occurrence of an emergency are:

1) notification of users to the information technology department employee in case of detecting an emergency situation in the operation of IS hardware and software complexes;

2) notification of employees operating the IS, who have detected suspicious changes in the system operation or configuration, to the system administrator and information security specialist;

3) systems for monitoring the status of the corporate information network, servers, user workstations, software, etc.

4) system logs that contain records indicating the occurrence or potential occurrence of an emergency situation.

## 2. General procedure in the event of an emergency situation

4. User, in case of an emergency situation listed in subparagraphs 2, 3,3,5,6, 7, 10, 11 of paragraph 2 of the instruction:

1) is suspending operations;

2) Immediately notifies the information technology employee;

3) informs the management;

4) resumes work only after authorization by the information technology employee for out-of-state situations listed in subparagraphs 2, 9 of paragraph 2 and after authorization by the information security specialist for subparagraphs 3,5,6,7,10, 11 of paragraph 2 of the instruction.

5. The system administrator conducts a preliminary analysis of the situation, if possible, promptly eliminates and notifies the supervisor and records the fact of occurrence of an emergency situation in the logbook of emergency situations (the form of which is given in **Appendix 1** to this Instruction).

6. In the event of an emergency situation that could seriously affect the implementation of the Organization's business processes, the IT employee:

1) reports the occurrence of an emergency situation to the first supervisor, and for emergency situations listed in subparagraphs 3,5, 6,7,10,11 also to the information security specialist;

2) determines the scope of the emergency situation, the size and area of possible impact;

3) shuts down affected components or switches to using redundant

resources;

4) restores serviceability of damaged critical hardware and other equipment, replacing failed units and assemblies with redundant ones, if necessary;

5) restores corrupted software using reference copies;

6) restores the necessary information using backups;

7) checks the operability of the restored system, makes sure that the consequences of the emergency do not affect further operation of the system;

8) notifies the first supervisor of the elimination of the emergency situation;

9) registers the emergency situation in the emergency situation logbook.

10) provides a report on the emergency situation to the system administrator.

7. Access to computer equipment for installation and configuration of software or replacement of network equipment shall be granted only to an employee of the Information Technology Department in accordance with his/her functional duties.

8. The IT employee who eliminated the emergency situation shall draw up an act describing the situation.

9. Each emergency situation is analyzed by an information security specialist. Based on the results of this analysis, proposals for possible organizational and technical measures to prevent future emergencies are developed and submitted to the management.

10.If necessary, by decision of the first manager of the Organization, an official investigation may be conducted on the fact of occurrence of an extraordinary situation in order to clarify its causes, assess the damage caused, identify the guilty parties and take appropriate measures.

## 3. Control of emergencies (crisis) situations and corrective actions on them

11. The procedure for notification of officials and deadlines for the implementation of measures in case of emergency situations are defined in the Plan of Measures to Ensure Continuous Operation and Restoration of Serviceability of Assets Related to Information Processing Facilities.

12. In order to perform preventive actions, the following activities shall be carried out in order to prevent the occurrence of emergency or crisis situations:

1) The system administrator shall monitor the Organization's information systems on a daily basis, including a survey of the status of DBMS, OS and RPO, using specialized software; in case of changes in the status of availability of information systems, the administrator will be notified in the "online" mode;

2) The system administrator shall monitor IS breach events on a daily basis and analyze the monitoring results;

3) The system administrator shall back up information in accordance with the information backup and recovery regulations;

4) In cases where information is received about possible impending

emergency situations, prompt notification of all involved persons and structures should be ensured.

5) The System Administrator shall report any information security events to the Information Security Specialist as soon as possible and make a corresponding record of the occurrence of emergency situations in the "Emergency Situations Log" document specified in Appendix 1;

6) each emergency situation should be analyzed by an information security specialist together with the system administrator.

13. The system administrator is responsible for monitoring the implementation of preventive actions to prevent emergencies or crisis situations.

14. A representative of the ISMS management is responsible for notifying the Organization's employees in case of emergency (crisis) situations and information security incidents.

15. For effective implementation of response measures in case of emergency situations, regular trainings on various emergency situations shall be conducted. Based on the results of the training, if necessary, this Instruction shall be clarified.

16. Collecting, storing and providing information on information security incidents in case an information security incident may lead to litigation in accordance with section 13.2.3 of ST RK ISO IEC 27002-2009

17. Registration of events related to the state of information security and detection of violations by analyzing event logs in accordance with the Unified Requirements of the Republic of Kazakhstan.

## 4. Peculiarities of actions in case of the most common emergency situations

18. If there is no communication with one or more servers located at the Provider, the system administrator shall immediately investigate the reasons for the lack of communication and further, if necessary, take measures in accordance with this Instruction.

19. In case of software failure, the employee of the information technology department finds out the cause of the failure. If it was not possible to correct the error by own efforts, including after consultation with the software developer, a copy of the report and accompanying materials (as well as files, if necessary) shall be sent by the information technology employee to the software developer.

20. If the password is compromised, the Rule on Organization Authentication Procedure should be followed.

21. If a computer virus is detected, the Organization's Rules for Anti-Virus Control must be followed.

22. When a server or network equipment fails, the system administrator must:

1) disconnect failed components of the server or network equipment;

2) take steps to immediately put in place a backup server or network equipment, if available, to ensure uninterrupted operation;

3) Analyze for loss and/or breach of data and software integrity;

4) check the operability of the damaged equipment;

5) restore operability of damaged components or services of server or network equipment (if necessary, restore software and data from backup copies with drawing up a report).

23. In case of detection of information loss or leakage on servers or personal computers of users, an employee of the Information Technology Department in the presence of the system administrator takes measures to search for and eliminate the causes of information loss (check the integrity and operability of software and computer equipment), if necessary, information is restored from backup copies. If information leakage occurred due to technical reasons, information security is analyzed, measures are taken to eliminate and prevent vulnerabilities.

24. In case of an intrusion attempt detected by the logging tools, the system administrator analyzes the information in the logs and, based on the analysis results, takes the following measures to prevent intrusion in case of a real threat of intrusion:

1) an unscheduled full password change is in progress;

2) An existing software update that addresses security vulnerabilities is applied.

25. When an NSD is detected, the following measures are taken:

1) the system administrator and information security specialist conducts an operational analysis of the circumstances of the intrusion, based on the results of which the first manager makes a decision on the possibility of continuing to operate the IS until the investigation of the incident is completed.

2) If necessary, the server is disconnected from the network or the server is stopped to check the IS and software for malicious code. Temporary transfer to a backup server is possible.

3) a copy of the system is created for further analysis by backup tools.

4) The system administrator analyzes the server logs and security logs.

5) unscheduled change of passwords that were related to the servers.

26. In case of communication channel failure, the system administrator notifies the communication service provider, works out the issue of communication channel restoration, and takes measures to switch to spare communication channels, if available.

27. In case of a power outage of more than 10 minutes, and if it is impossible to use uninterruptible power supply sources, an employee of the Information Technology Department must correctly shut down all servers and network equipment. In case of power supply in the building of the Organization, the system administrator together with the information security specialist shall analyze the presence of loss and (or) destruction of data and software on the server, as well as check the operability of the equipment. If necessary, the software and data are restored from the latest backup copy, and a report is drawn up.

28. If a power failure is detected in equipment located in the Provider's office or on the Provider's premises, the information technology employee shall immediately notify authorized employees. If the estimated time of elimination of power failure exceeds 30 minutes, the information technology employee shall notify the first supervisor. Upon resumption of power supply, the system administrator shall carry out measures to verify the integrity of the equipment and software.

29. In the event of a natural disaster (earthquake, flood, hurricanes, fires, etc.), system administrators should ensure that the last complete copy of the system is preserved as much as possible.

30.To develop clear actions of employees in case of disasters, the information security specialist should organize special training drills at least once a year.

## 5. Business continuity and recovery tools

31. The risks of technical emergencies are considered within the scope of this Instruction.

**Risks of man-made and natural disasters are referred to Emergencies and are discussed in the document: "Rules for ensuring continuous operation of assets related to information processing facilities".**

32.The means of ensuring continuous operation and recovery is:

1)backup of the Organization's software and information resources;

2)uninterruptible power supplies on server machines

33.Backup provides information recovery in case of information loss. Backup copying is performed in accordance with the requirements of the Regulations on Information Backup and Restoration.

34.Uninterruptible power supplies provide the connected equipment with some battery life, in case of disconnection or the parameters of the electric current exceeding the permissible parameters.

## 6. Responsibilities and actions of information systems business continuity and recovery personnel

35. The actions of personnel in a crisis situation depend on the severity of the situation.

36.In the event of a threatening or serious critical situation, personnel actions include the following steps:

1) immediate response from responsible personnel;
2) partial restoration of serviceability and resumption of processing;
3) full system recovery and resumption of full processing;
4) investigating the causes of the crisis situation and identifying those responsible;

5) During the daytime, an employee who has detected an emergency (crisis) situation must inform his/her immediate supervisor and system administrator orally, the information security specialist orally and, if necessary, in writing;

6) development of solutions to eliminate the causes and prevent similar violations in the future.

37. The organization informs the organization providing building security of the following necessity: in the event of an emergency situation at night, the security officer responsible for security should inform the responsible employee of the IT department.

38. Employees operating the IS are obliged to notify the information security specialist of all observed preconditions for the emergence of emergency situations.

39. The organization of work in crisis situations is carried out by the system administrator and information security specialist assigned to them.

40. Control over the organization of work in crisis situations is exercised by the Head of the Organization.

## 7. Control of emergencies or crisis situations and corrective actions on them

41. The following functions are used to control the occurrence of emergency situations:

1) registering the occurrence of emergency situations in the emergency situations logbook;

2) drawing up acts, describing the emergency situation and corrective actions, attaching explanatory materials (screenshots, printouts of the event log, etc.), documented, confirming their authenticity.

## 8. Responsibility

42. Management and maintenance personnel responsible for the performance of the IS are responsible for:

1) improper fulfillment of their functional responsibilities;

2) failure to ensure proper conditions of safety, accessibility, confidentiality of processed information, within its competence.

43. At least once every six months, the system administrator analyzes the incidents recorded in the emergency log to develop preventive measures to reduce the risk of repeated emergencies.

44. Persons who violated the requirements of this instruction shall be brought to disciplinary or other responsibility in accordance with the current legislation of the Republic of Kazakhstan.

## 9. Control over compliance with the Instruction

45. Compliance with this Instruction is monitored by the system administrator and information security specialist.

46. For violation of the norms stipulated by this Instruction, disciplinary sanctions may be applied to the Organization's employees upon recommendation of the Information Security Specialist, based on the materials of official investigation.

Annex 1
to the Instruction on the procedure for user response to information security incidents and in emergency (crisis) situations

"__"_____202_ № ____

## Logbook for registering emergency situations

| No. n/a | Date | Brief description of the emergency situation | Start time | End time | Simple | Reason | Method of elimination | Responsible |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

**FAMILIARIZATION SHEET**

| № | Surname, first name, patronymic | Position | Personal signature | Date |
|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |