

HJ

INDUSTRY STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

HJ 729-2014

Security specification of environmental information system

环境信息系统安全技术规范

(English Translation)

Issued on: December 25, 2014

Implemented on: March 1, 2015

Issued by: Ministry of Ecology and Environment

Table of Contents

Preface .ii
1 Scope of application
2 Normative reference documents
3 Terms and Definitions
4 Protection object .2
5 Safety objectives
6 Overall safety architecture
7 Information security protection method
8 Physical security .7
9 Network security .9
10 Host Security
11 Application safety
12 Data Security and Backup Recovery

Foreword

To implement the "Environmental Protection Law of the People's Republic of China" to promote environmental information work, strengthen and regulate the environmental letter Safety system construction and management, to ensure the safety of environmental information systems, the development of this standard.

This standard specifies the physical security of the environmental information system, network security, host security, application security, data security and Backup and recovery, system construction, system operation and maintenance, terminal and office security aspects of security requirements.

Appendix A and Appendix B of this standard are normative and Appendix C is an informative appendix.

This standard is released for the first time.

This standard is organized by the Ministry of Environmental Protection Science and Technology Standards Division.

The main drafting of this standard. the Ministry of Environmental Protection Information Center, Beijing Shenzhou Green UNITA Technology Co., Ltd.

The Environmental Protection Department of this standard approved on December 25,

2014.

This standard is implemented on March 1, 2015.

This standard is explained by the Ministry of Environmental Protection.

Environmental Information System Security Technical Specification

1 Scope of application

This standard specifies the physical security of the environmental information system, network security, host security, application security, data security and backup recovery, System construction, system operation and maintenance, terminal and office security requirements.

This standard applies to the national environmental protection business network within the environmental information system planning, design, development, operation and maintenance of the various stages segment.

2 Normative reference documents

The contents of this standard refer to the following documents or their terms. For undated references, the valid version applies to this standard.

Information technology - Glossary GB/T 5271.8-2001 Classification of safety information for computer information systems GB/T 17859-1999 Information security technology - Network - based security - Technical requirements GB/T Information security technology - Information systems - General safety technical requirements GB/T 20271-2006 Information security - Technical information systems - Safety engineering management requirements GB/T 20282-2006 Information systems - Disaster recovery specification GB/T 20988-2007 Information security - Technical information systems - Physical safety - Technical requirements GB/T Information system - Security level - Basic requirements for protection GB/T 22239-2008 Information security - Technical information systems - Safety - rating - Guidelines for the protection of grading GB/T 22240-2008 Information security - Technical information system - Level protection - Safety design - Technical requirements GB/T 25070-2010 Code for design of power supply and distribution system GB/T Code for design of room for electronic information system GB/T 50174-2008 Guide for Environmental Information Standard

3 Terms and definitions

GB/T 5271.8-2001 Section VIII. Terms and definitions established in safety, and the following terms and definitions apply to this standard.

3.1 Information system information system

The sum of the entire infrastructure, organizational structure, personnel, and components used to collect, process, store, transmit, distribute, and deploy information.

3.2 Information system security information system security

Use reasonable security measures to protect information from information systems that are not accessed by unauthorized users during storage, processing, or transmission, and to ensure that authorized users can use the system properly.

3.3 Confidentiality

The nature of the data, indicating the extent to which the data is not provided or not disclosed to an unauthorized person, process, or other entity.

3.4 Integrity

To ensure that information and information systems are not intentionally or unintentionally altered or destroyed.

3.5 Availability

To ensure that information and communication services can be used as expected.

3.6 Security domain security domain

A logical range or area where the information units in the same security zone have the same or similar security level or security requirements the administrator of the security service defines and implements a unified security policy. It is an area that is divided from the point of view of the security policy.

Threatening threat

From outside the information system, through unauthorized access, destruction, disclosure, data modification and/or denial of service to information systems any environment or event that causes potential harm.

3.8 Risk risk

The performance is a possibility that is determined by the likelihood of a threat, the adverse effects that can be caused by the threat, and the severity of the impact.

4 Protection object

Environmental information system security protection object, including the national environmental protection business within the scope of the network of information networks, business systems, environmental information and its physical environment, supporting infrastructure and safety equipment and so on.

4.1 Environmental Information Network

Environmental information system security protection network object is the national environmental protection business network within the scope of the various information networks, national environmental protection Business network, including national, provincial, city, county four, network structure shown in Figure 1.

Figure 1 Schematic diagram of the network structure of the environmental protection business network

4.2 Environmental Information Application System

Environmental information system security protection business object is the environment information system to run various types of environmental business application system, according to HJ 511-2 009, environmental information system according to business application type can be divided into environmental protection core business application system and integrated application system two categories, including.

A) Environmental protection core business applications include environmental monitoring management, pollution monitoring and management, ecological protection management, nuclear safety and radiation Management, environmental emergency management information system. The role of each system are.

1) Environmental monitoring management information system for the realization of the national environmental quality data (including ambient air, surface water, groundwater, Sound environment, coastal waters, acid rain, dust storms and other data) management, and covers ecological monitoring, pollution monitoring and other business;

2) pollution control management information system covering pollution control management, environmental monitoring and management and environmental impact assessment and environmental statistics, etc.

business;

3) Ecological protection management information system covers regional ecological environment management, rural environmental protection management, biodiversity conservation and so on Service

4) Nuclear safety and radiation management information system covers nuclear facilities