



SECURITY POLICY

PUBLIC

2008-09-15

Author:
Jevgenij Kaplanas

Version 2.2

1 (11)

BALTIC DATA CENTER

SECURITY POLICY

Version: 2.2

Version control:

<i>Version</i>	<i>Date</i>	<i>Author</i>	<i>Changes</i>	<i>Approved by whom and when</i>
1.0	2006.07.05	Gediminas Pilipavičius	First version of document	General Manager Order No. IS-1678 2006.08.03
2.0	2007.06.15	Jevgeij Kaplanas	Complemented security principles	General Manager Order No. IS-2007.06.
2.2	2008.09.15	Jevgeij Kaplanas	Minor complements and changes	General Manager Order No. IS-2008.09.

CONTENT

1. SCOPE	3
2. DESCRIPTION OF INFORMATION SECURITY	3
3. EXCEPTIONS TO THE INFORMATION SECURITY POLICY.....	3
4. OBJECTIVE OF INFORMATION SECURITY.....	3
5. ELEMENTS THAT GUIDE INFORMATION SECURITY OPERATIONS.....	4
6. THREATS ON SECURITY.....	4
7. CUSTOMER AND SERVICE PROVIDER RESPONSIBILITIES.....	4
8. COMPANY LEVEL SECURITY MANAGEMENT	5
8.1 Risk management committee	5
8.2 Unit Level Security Management	6
8.3 Managing Security Related Incidents.....	6
8.4 Management of Security incidents reports.....	6
8.5 Prioritization of Security Measures.....	6
9. PRINCIPLES OF SECURITY	6
9.1 Personnel security	6
9.2 Security training	7
9.3 Physical Security.....	7
9.4 Business Continuity Management.....	8
9.5 License, Hardware and Software Management.....	8
9.6 Systems Maintenance	8
9.7 Media Handling and Security.....	8
9.8 Access Control.....	8
9.9 User Identification and Password Management	9
9.10 Asset Classification and Control.....	9
9.11 Protection against Malicious Software	9
9.12 Information Exchange using Network.....	9
9.13 Compliance	9
9.14 Action against cybernetical crimes	10
9.15 Following the law and rules demands.....	10
10. MAIN PRINCIPLES OF SECURITY IMPLEMENTATION.....	10
11. SECURITY IMPLEMENTATION RESPONSIBILITY AND LIABILITY	10
12. MAIN PRINCIPLES OF INFORMATION SECURITY IMPLEMENTATION.....	11
13. INFORMATION SECURITY IMPLEMENTATION RESPONSIBILITY AND LIABILITY	11
14. THE EFFECTIVE DATE OF THE POLICY	11

Baltic Data Center Security Policy

1. SCOPE

Company security - very important part of Company business by striving for Company business goals. Company security goal is to create and keep the optimum business conditions for Company business, protect its activities, universally manage threats. We strive for Company security by constantly improving and implementing Company Security Policy.

Information security is achieved by implementing proper set of maintenance methods that contain policies, procedures, rules. These maintenance methods are implemented by striving to ensure that special security goals of organization are underway.

Baltic Data Center Security policy (later in this document referred to as Security Policy) defines the mandatory security baseline to be followed within the company. The policy is further defined in company approved Security Rules, instructions, procedures that are mandatory and Guidelines that are recommended to be followed.

All company security documents are written in Lithuanian. The Security Policy is classified as public and therefore available to all Company personnel, subcontractors and partners. Security Rules, instructions, procedures and Guidelines are classified as internal and therefore only available for company personnel, in case it is specified in different way.

2. DESCRIPTION OF INFORMATION SECURITY

Information security – activities dedicated to ensure confidentiality, integrity and availability of data transfer and usage.

Confidentiality means that information is accessible only to those authorized to have access.

Integrity means safeguarding the accuracy and completeness of information in all stages of its processing as defined by owner of information.

Availability means ensuring that authorized users have access to information and associated assets when required.

Information security implementation rules are presented in section 11.

3. EXCEPTIONS TO THE INFORMATION SECURITY POLICY

Exceptions to the information security policy shall apply if strict adherence to the safety regulations or procedures:

- significantly reduces efficiency of the resource or has negative impact on service quality;
- requires significant financial expenses;
- is far too complicated in technical sense;
- requires unacceptable period of time.

4. OBJECTIVE OF INFORMATION SECURITY

Information security aims at the continuity of business operations in all circumstances. Our products, services and internal operations must comply with legislation. We have to fulfill customer and other interest group demands and expectations on security. Therefore every Company employee has a personal responsibility for security on his/her behalf.

The absolute precondition of Baltic Data Center's operations is the ability to be regarded as a reliable and reputable partner. The maintenance of this reliability and good reputation requires that the Company operates in accordance with laws, statutes and orders by authorities and that it can fulfill all the obligations placed on it by agreements and general business practices.

Due to this, guaranteeing sufficient information security is regarded as a generally accepted obligation.

To achieve our security goals one of the main principles is **continuous improvement of security**.

Actions on security improvements are carried out based on innovations in security area and risk analysis results of company assets used for provisioning of services.

5. ELEMENTS THAT GUIDE INFORMATION SECURITY OPERATIONS

A considerable number of laws regarding information security govern the Company and its customers' operations. Security Policy is based on requirements of Lithuania Law and internationally accepted documents the main of which are ISO 27001:2005 standard and European Union issued its information security directive 12 July 2002 (2002/58/EU). In addition to laws and statutes, the agreements between Baltic Data Center, customers and suppliers/subcontractors and partners have a very central position, as the Company must be able to follow their terms. In addition to this, the Company has to follow unwritten customer and interest group rules and expectations to be regarded as a secure IT services provider.

6. THREATS ON SECURITY

There are several different threats placed on security. Only some of these are threats actually directed to information technology. The threats can roughly be divided into the following four categories.

1. Loss of confidentiality, integrity or availability (thefts, deliberate damage and industrial espionage, crisis that threatens society) based on actions of not a company employees
2. Threats directly related to Company employees
3. Technical threats directed to physical environment; for example fire, water damage, disturbances in electricity distribution etc.
4. Natural forces (exceptional environmental conditions and natural phenomena)

Company security management follows development in the threat categories. Security Policy, rules, procedures, instructions and guidelines are updated to correspond with the development.

7. CUSTOMER AND SERVICE PROVIDER RESPONSIBILITIES

Baltic Data Center is an IT service provider for internal and external customers. The owner of an information system is primarily responsible for defining the needs to protect the information or the information system. The Company must make sure that the information system owner knows his/her responsibilities. As an IT service provider, Baltic Data Center is responsible for carrying out sufficient security measures that meet the existing customer and internal needs. Legislation may place a similar responsibility of information protection on the service provider as on the owner.

8. COMPANY LEVEL SECURITY MANAGEMENT

The Company management decides on all security principles at Company level. The Company management appoints an employee for overall responsible for Security at Company level and his/her deputy. Responsible for Security employee reports to Company management.

The Responsible for Security employee owns this Security Policy. The policy is reviewed at least annually. The Responsible for Security employee is responsible for:

- General coordination and instructions related to security within the Company.
- Investigation and reporting on security related incidents to the Company management.

An Responsible for Security employee has the right:

- to convene a meeting of the risks management committee;
- to restrict user's rights to information if it endangers safety of the latter;
- to submit his/her conclusions to the management about the safety incidents that took and/or may take place;
- to co-ordinate work of safety assurance teams formed;
- to obtain information from employees regarding information safety and its breaches;
- to assign tasks to the managers aimed at improvement of information safety condition.

Baltic Data Center General Manager is responsible for implementation of Security Policy within the Company.

Risk related elements evaluation and management is carried out by using PDCA model: Plan, Do, Check, Act.

8.1 Risk management committee

On Risk management committee are Responsible for Security employee, Finance Director, General manager and Unit directors. Chairman of Risk management committee is Responsible for Security employee. Risk management committee is a common body for escalation and resolution of security matters.

Risk management committee convenes at least two times a year.

Usually in this committee following matters are discussed:

- reviewing and approving information security policy and overall responsibilities;
- monitoring significant changes in the exposure of information assets to major threats;
- reviewing and monitoring information security incidents;
- approving major initiatives to enhance information security.

When necessary, the Company management or the Risk management committee can appoint special teams responsible for maintaining continuous preparedness regarding some aspect of the security area.

8.2 Unit Level Security Management

Unit director is responsible for the supervision of security in his/her unit. Each Unit is responsible for information security of the systems it uses for work. Unit director is responsible for reporting of security incidents to responsible for Security employee according to Security incidents handling procedure.

8.3 Managing Security Related Incidents

Security related incidents require fast response from the organization to prevent the incident from growing out of control. Responsible for Security employee is responsible for company internal investigation process.

Company Public Relations employee is responsible for incident/crisis communication.

Baltic Data Center has a multi-level incident/crisis management organization. Main principle is that incidents should be managed locally if possible. Unit directors are responsible for solving of incidents/crisis that took place in their units. The management responsibility is escalated to higher level depending on nature of the matter. Permanent part of the security incident management organization is company level Crisis Management Team who takes responsibility only in extreme cases. Security incident management process is described in the company Security Incidents Handling Procedure. The procedure covers also crisis communication issues.

8.4 Management of Security incidents reports

The Company responsible for Security employee draws up a summary of the security reports every six months for the Company management. This summary is one of the inputs for continuous security improvement process.

8.5 Prioritization of Security Measures

When making decisions on the order of security measures, the following order apply:

1. protect human life and the health of individuals
2. protect confidential or other especially important information
3. protect other information
4. prevent damage to systems
5. protect the usability of systems.

9. PRINCIPLES OF SECURITY

9.1 Personnel security

Each Baltic Data Center employee is obliged to follow the policy and instructions given on security and report to his superior about the problems, threats or lines of action that are contrary to the instructions that he/she has detected.

Each employee must sign Company non-disclosure agreement (it is included as part of Internal Working rules) that is valid also after the termination of employment.

Non-disclosure agreements are also required from subcontractor or partner employees, consultants or any personal/legal entity working for Baltic Data Center. Company non-disclosure agreements state that the implication of Professional secrecy has been clarified. Agreements of not public items must be used in all cases when confidentiality's, secrecy's or information revelation is assigned for owner (or for superiors). Organization's letterforms, printed forms and other documents must be properly supervised in case to avoid inadequate usage.

Both physical and electronical key's lending is prohibited. This obligation must be involved in employment contract.

Money lending for associates must be strictly controlled.

All the employees must obey the organization's information security rules. Any information security incidents which arise for not obeying the rules must immediately take disciplinary actions.

Each employee may be subject to background checking (biography, education, qualification) at appropriate level. The methods used in checking depend on employee work assignments, access to information and legislation. Subcontractor or partner employees and consultants may also subject to background check depending on work assignments.

9.2 Security training

Basic security training must be a part of employee induction training. Security Policy, Rules and instructions must be known and communicated to all employees. The level of knowledge needed depends on work assignment. This also applies to subcontractors and partners.

When personnel members change work their information security requirements must be repeatedly valued and necessary training provided.

Permanent employees must be informed about the ways to warrant information security which would help to raise the knowledge and recognize potential threats to protect from it properly.

Niche and technical staff must be properly trained and prepared for work with new systems and provided with knowledge about new system functioning and it's appliance in practice.

Unit director is responsible for ensuring that his/her employees receive proper labour and health security training and training what to do in case of fire.

9.3 Physical Security

Physical protection is achieved by creating one or more physical barriers around the organization's premises and information processing facilities. The use of multiple barriers gives additional protection. Company use physical barriers in order to protect areas where information processing facilities are located and company employees work. Location of each barrier and reliability depends on results of risk evaluation. In-depth information on premises security is found in BDC Premises Security Rules.

Persons, employees as well as visitors, who visit in the Company premises, must be possible to identify. All employees must wear a photo ID-badge and all visitors must wear a visitor badge. For authentication purposes, the photo on the ID-badge must be identical with the photo stored in the Company internal directory. Baltic Data Center employee is responsible for visitors entering and leaving the office.

Photography and/or video/sound recording inside BDC office without a permit is prohibited. This rule includes also the use of other equipment having this capability (mobile phones etc) for this purpose.

The protection provided should be proportional to results of identified risks. In order to reduce risk of unauthorised access or possible damage to papers, removable storage media and information processing facilities, the clear desk policy is recommended, i.e. not allowed to leave important documents and removable storage media on desk without supervision.

All the employees must know that they must question all the strangers which appears in organization's premise.

9.4 Business Continuity Management

The Company has prepared itself in advance for a deliberate or unintentional breach of information security. The procedures described in the company Security Incidents Handling Procedure must be followed when information is distributed in unusual conditions or crises.

Threats on central company Information and Communication Technology infrastructure are managed according to company Security Incidents Handling Procedure. Units must define and document the measures taken when crucial for a business specific information system is an object of a security attack or threat. Units are responsible for ensuring that appropriate number of employees is available in crisis situations to fulfill customer demands. Contingency plan must be periodically revised for the guarantee that administration and staff knows how to pursue it.

9.5 License, Hardware and Software Management

The Company must comply with software/hardware license agreements. All hardware and software used in Company information architecture must be acquired from a reliable source and suit company's security requirements..

9.6 Systems Maintenance

When designing information security arrangements, required level of information security, system usability and the costs arising from information protection must be balanced. Arrangements that are unnecessarily strict should not be used, if these lead to unnecessary costs or if they make the systems too complicated to use. All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services. Qualified engineers must provide company's licenced, bought or leasehold software with appropriate maintenance implements.

9.7 Media Handling and Security

The level of securing information must be taken into consideration in all the stages of information processing. The information must be stored in data media providing an appropriate level of information security, and these must be kept properly. In detail it is described in Information Media Handling Rules document.

9.8 Access Control

The information systems users have the right to access only such files, data media, systems and other resources they are entitled to use due to their work assignments. These access rights and their supervision should be managed with technical arrangements always when this is sensible with regard to the entity. The fact that a resource is not technically protected for some reason does not give unauthorized users the right to access this resource. All computer equipments or terminals must protect stored data with log-on password.

Examples of how this protection can be accomplished are:

- automatically activated, password protected screen saver
- automatically logging off the user after defined inactivity period
- or other means that lock the platform when it is not being used.

9.9 User Identification and Password Management

The user codes, passwords, identification devices, photo ID-badges and other corresponding material given as support for user rights are personal, unless explicitly defined otherwise. It is not permissible to give personal material to others even for temporary use. Regulations related to information security instructions, for example, changing the password regularly, must be followed even when the technology used does not especially force the user to do this.

9.10 Asset Classification and Control

Company information assets must be classified and protected according to company Information Classification and Handling Procedure. Basic classification level for customer information assets is confidential.

Units are responsible for protecting internal information, trade secrets or confidential information from unauthorized access. This obligation to protect information includes both physical data protection (external persons visiting company premises or working there) and logical data protection (accessing the data through a network).

9.11 Protection against Malicious Software

All equipment connected to the network used by the Company must be equipped with proactive virus protection solution. Units are obliged to protect the systems they are responsible for against viruses and other risks of damage. Used networks must be protected with technical arrangements (firewalls, IDS systems, VPN infrastructure etc) to control access from non-trusted networks.

It is necessary to implement and maintain procedures intended for analyzing warnings of "false" viruses.

9.12 Information Exchange using Network

Email system used by the Company and Internet connection is intended for Company business usage.

Small scale private email usage is allowed. Email is considered as personal and confidential, and the basic principles of letter mail privacy are applied to it. It is not permissible to send unprotected confidential information through email when there is an evident risk of information leakage due to technical or other reasons.

Email and Internet usage rules are defined in Company level documents: Electronical catalogs rights maintenance rules and TEO IS Security Policy.

9.13 Compliance

A Company or customer employee is obliged to follow both Baltic Data Center Security Policy and the security and operation policy of an external organization when he/she uses data communications network to access resources governed by this external organization. Each Unit is responsible for following information security within the Unit. Faults and deficiencies detected in the security audits or tests shall be remedied as soon as possible. Temporary measures in certain cases can be required immediately.

Responsible for Security employee together with his/her deputy will review the security measures taken by the Units. Violations against this policy will be investigated and interpreted as violations on contract of employment.

9.14 Action against cybernetical crimes

The highest level security is necessary for network.. Employees which are responsible for network's and external communication must be prepared to evaluate the risk and create defence systems which would reduce the threat of cybernetical crime as much as possible.

Action plans must be prepared, supervised and regularly revised, they should warrant that the damage of already occurred cybernetical crimes would be reduced as much as possible and that reconstruction would be performed as soon as possible.

The performers of cybernetical crimes must be procesuted by law. It is necessary to settle appropriate procedures for warrancy of proper accumulation of evidences and their protection.

9.15 Following the law and rules demands

Organization plan fully perform data security laws as much as it directly influence company's work.

Employees are prohibited to write abusive comments about other persons and organizations. Information from internet or other electronical sources can be prohibited to use or forward without permission of copyrights owner.

A text from a reports, books or documents can be prohibited to duplicate or use without permission of copyrights owner.

10. MAIN PRINCIPLES OF SECURITY IMPLEMENTATION

- Each Company employee depending on his/her position take part in creation, implementation and improvement of Company security processes.
- Company follows Security Policy, Rules and Procedures. Company security documents improvements or updates are announced in units meetings, security trainings or Company meetings. Urgent changes are communicated by e-mail.
- After notice of Company security breaches, each employee depending on his/her authority must eliminate them.
- Every case related with Company security breaches must be registered and line manager must be informed.
- Company management should be regularly informed about eliminated breaches.
- Each Company unit investigates and analyses tthreats related to Company security in its business areas and improves its activities based on anglysis results
- Each manager traces news and development in security areas locally and abroad related to his/her business area.
- Each division cooperates and develops cooperation with the most important interest groups in security areas.

11. SECURITY IMPLEMENTATION RESPONSIBILITY AND LIABILITY

Each employee is responsible for Company security in his/her surroundings. Everybody must follow orders, instructions and rules related to security. Every breach of security should be reported to his/her superior immediately.

Company divisions managers respond for sufficient carrying out, improvement and supervision of Company security functions in their divisions. Their goal is to make such Company business environment that threats for Company employees, business, assets and customers would be minimal.

General manager respond for implementation of Company Security Policy.

12. MAIN PRINCIPLES OF INFORMATION SECURITY IMPLEMENTATION

- All Company information and data has an appointed owner. They are accessed, used and distributed only in regulation way and should be protected according to minimal security level set-up requirements if not stated in onother way.
- Owner of information and data or his deputy clasifies data, information depending on its importance and defines accurate security levels. Information, data, information transfer systems are protected and used according to defined requirements set by him.
- Owner of information or his deputy grants access to information which is responsible for only to those persons who need it for work assignments.
- Divisions make contingency plans and regular update them in order to secure continuos operation of systems in case of unusual or emergency situations.
- Company should be guarded against computer viruses. Effective antivirus solutions should be created, implemented, maintained, updated and improved.

13. INFORMATION SECURITY IMPLEMENTATION RESPONSIBILITY AND LIABILITY

Each Company employee is responsible for ensuring that only authorised persons could use information, data and systems.

Each user of internal computer network is allowed to use personal computer, computerized work place and information systems only after proving his identity by personal password.

Each employee is responsible for constant update of antivirus programs in personal, portale and home-located computers used for work purposes.

Each user is responsible for ensuring that information, data, data transfer and information systems are used only for work assignment to carry out.

Manager of each user is responsible for ensuring that employees use information, data and information systems only according to defined rules and only that much what is needed to perform his duties.

Each owner and administrator of information, data, information systems is responsible for ensuring that user could use information, data, data transfer systems only according to defined rules and that he could Access only that information which he has authority to Access.

14. THE EFFECTIVE DATE OF THE POLICY

This new version of Company Security Policy will come into force on 15.09.2008. It succeeds the previous version of the policy.