Overarching policy

Using ISO 27002 as the basis this policy will be a high level security policy to protect the information assets of Eastchange. The parts chosen to be included in this policy covers the most important gaps identified during a security analysis of Eastchange. In the below listed points the most important aspects are listed. This policy may be revised and expanded as needed in the future to accommodate changes within the company and in the threat landscape.

Definitions:
Company: the ‘company’ refers to Eastchange.
Information security: as defined by ISO 27000, the preservation of confidentiality, integrity, and availability of information
User: authorized user who have been allowed access to necessary parts of the system to perform their work tasks.

Define and decide roles and responsibilities
In order to protect the information of the company roles need to be decided so that responsibility regarding the protection of all information assets is assured. An information security manager should be appointed to hold overall responsibility for development, implementation and support of information security.

The CISO (Chief Information Security Officer) would be responsible so that the company security policies are followed. The CISO would also be responsible for information security incident management.

The director of IT would be responsible for backups and recovery.
The director of HR would be responsible for HR security.
Access control is decided by role by HR and approved by the director of IT.

These roles may further delegate day-to-day tasks but they hold the final responsibility for making sure that the relevant policies are followed.

Human resources policy
Responsible role: the director of HR.

Background checks and vetting are required to ensure that new hires are trustworthy and allowed to work within the field, and would not pose a risk to the company. Verification of relevant studies and curriculum vitae is also required.

Training and education of the information security policy of new and existing hires is also part of this responsibility in order to ensure that users follow proper company information security behavior. Disciplinary action is taken according to policy when breach of policy has been confirmed.

More details can be found in the Human resources policy.

Access control and Physical and environmental security
Responsible role: the director of HR with the director of IT confirming

To protect the information assets of the company no user should be granted more access or privilege than they need for their work tasks. In order to secure assets and facilities HR decides what access a user should have with IT implementing it. This is to implement segregation of duties in order to ensure that no one is granted undue access.

Access can be both logical and physical and should be handled the same. Access cards are the main means for access control with keys available as backup, stored securely. All access cards are personal and to be carried at all times while on company premises.

More details can be found in the Access control and Physical and environmental security policy.

Cryptography
Responsible role: director of IT

Best practice and standards should be followed when implementing cryptography, key management and recovery options.

Disks with sensitive data should always be encrypted, as well as any device with company data that would leave a controlled and secure environment.

More details can be found in the Cryptography policy.

Backup
Responsible role: director of IT

Backups should be made regularly and encrypted, backups should be stored off-site from the main facilities and be tested regularly to ensure they work as intended.

More details in the Back-up and recovery technical policy.

Information security incident management
Responsible role: CISO

In case of an information security incident processes and procedures for preparing, handling, responding, recovering, reporting, and revising are needed. These processes need to be clearly defined with clear responsibility and roles attached.

More details in the information security incident management policy.

Detailed, Technical Policy: Back-up and recovery technical policy

Purpose
In order to protect against hacking and ransomware attacks, natural disasters, employee errors, and corrupted data, a policy regarding the backup and recovery of lost data is required. This policy will be based on the standard ISO/IEC 27002 for the code of practice for information security controls.

Backup Strategy
The local system that the employees will be working on will be located at the main data centers on Renstiernas gata in Stockholm. These servers are where the employees will complete most of their work and should only store data pertaining to the company and their work. A small backup server will be located at this office in case of employee errors that can quickly be fixed.

The previous data center used in Sundbyberg that was moved to Renstiernas gata, will act as a local backup data center. Allowing for quick, nearby access in case there is a local problem at the Renstiernas gata data center.

Lastly, back ups will be placed in the off-site data center located in Luleå. This will mean that the Luleå data center will act as an off-site data center for the existing Bitflip AB and Eastchange AB. This protects the business in case there is some sort of natural disaster in the Stockholm region because data is handled at a sufficient distance.

Data Backup Procedures
Whenever data is being backed up, accompanying records should also be added to the backed up data. These records must state: where the backup is coming from, when the backup is being made, the size of the backup, whether it is an automatic or manual backup, and if it is manual who authorized it, the hash of the backup, and time the record was last modified.

All data that is backed up must be encrypted using a symmetric key encryption that will be randomly generated, and securely stored in the head office and stored off-site at the Luleå data center in the case of an emergency. Symmetric keys are used because it will make the encryption process more efficient than using an asymmetric key encryption, and because no outsiders need to know or send encrypted messages to the company. However, this places more importance on storing the symmetric key safely, and out of reach from unauthorized personnel. The only exception are the VM snapshots that are taken every hour and stored at Renstiernas gata, which does not have to be encrypted when storing them.

To ensure that the backup files are safely received, all the traffic between the data centers must be encrypted and the communication channels must be secure, in order to prevent malicious actors from intercepting the data.

1. Virtual Machines (VM)
    - VM snapshots will be stored in the local backup located at Renstiernas gata
    - Full backups from VMs will be sent to the local backup storage as well as the storage located in Sundbyberg data center

2. Physical Servers
    - Backups must be made to the data centers in Sundbyberg and in Luleå (secondary)

3. Clients
    - All employees will be required to backup their daily generated data to the local backup server

Backup Schedule

1. Virtual Machines (VM)
    - Full backup of VMs will be made every 24 hours
    - Incremental backups shall be made every 8 hours during the day
    - VM snapshots will be taken every hour
2. Physical Servers
    - Full backup of the server shall be made every 24 hours to the Sundbyberg data center
    - Incremental backups will be made every hour
    - A weekly backup will be made to the Luleå data center

3. Clients
    - Clients backup their data once a day at the end of the office hours

Data Recovery

1. Virtual Machines (VM)
    - VMs that are stored in the local server can be collected and reinstalled within one hour upon a failure occurring.
    - VMs that are stored in the Sundbyberg server can be reinstalled to the employee within two hours upon request, with possible loss of data from desired backup
    - VMs that are stored in Luleå should be able to be reinstalled to the employees system within three hours of the request for the specific VM
    - Should a VM which is not the most recent one be requested, then a new branch of save files shall be started
2. Physical Servers
    - There will be standby servers ready to be deployed using backup data from current running servers
3. Clients
    - Shadow Copies (VSS) is enabled by default for immediate recovery on local drives and shared folder accessed as a mounted drive on the client device

- Data from virtual machine backups can be restored from either daily full backups or 8 hour incremental backups by arrangement of

Data Retention

1. Virtual Machines (VM)
    - Full backups taken on weekend(Saturday) will be kept for 1 week.
    - Full backups taken on the last weekend of the month will be kept for a month
    - Full backups taken on the last weekend of the quarter will be kept for 3 month
    - Full backups taken on the last weekend of the year will be kept for a year
    - Every other full backups will be disposed after 6 days
2. Physical Servers
    - Full backups taken on weekend(Saturday) will be kept for 1 week.
    - Full backups taken on the last weekend of the month will be kept for a month
    - Full backups taken on the last weekend of the quarter will be kept for 3 month
    - Full backups taken on the last weekend of the year will be kept for a year
    - Every other full backups will be disposed after 6 days

3. Clients
    - Full backups taken on weekend(Saturday) will be kept for 1 week.
    - Full backups taken on the last weekend of the month will be kept for a month
    - Every other full backups will be disposed after 6 days

Applicability

The policy will apply to all data and records pertaining to the company and their clients. All employees must understand the policy and follow it without fail.