IT Access Control Policy

Rev.	Issue for use	Doc. Title
B	Description	COMP-IT Access Control Policy

Prepared by	Checked by	Approved by
Silvan Penglou (Head IT)	Patrick Kahl (CEO)	Benjamin Ringsbacher (Group)

Version	Change Date	Approved by
1.1	20130212	Patrick Kahl (CEO)

1. Policy Statements (Access Control)

- There is no access without a strictly control. All access must be controlled by a formal written registration and de-registration process.
- A detailed control of access is possible due to the use of individual user accounts. The use of generic accounts must be prohibited.

2. User access

2.1 Account privileges

Only necessary access to perform the work out of responsibilities of their role and function should be guaranteed. Segregation of duties must be always in place. High privileged user accounts such as administrators must be strictly controlled and restricted to only those users who are responsible for management or maintenance of information systems. Administrators must have a separate user account apart from their standard user account which shall only be used for administrative processes. If an employee with a higher privileged account leaves the company, the administrator passwords needs to be changed.

2.2 Password Management

2.2.1 General rules

Passwords, as well as initial passwords, must follow the following rules:

- It must be frequently changed
- It must contain a minimum length
- It must be a combination of alpha and numeric characters
- Password complexity must be enforced
- The delivery of new passwords must be secured

2.2.2 Password Requirements

Criteria:

- User Passwords are at least 8 characters long
- High privilege passwords are at least 12 characters long
- Passwords must contain a combination of letters, numbers and special characters as well as password complexity (e.g. lowercase, uppercase) must be enforced
- Passwords must be changed every 90 days
- Password history is in place and the last 10 passwords shall not be used
- All passwords are masked during input and encrypted during transmission and storage
- Logins are automatically locked after 5 failed login attempts
- Enable automatic unlock off locked user at midnight must be deactivated
- Sessions end automatically after 3 failed login attempts
- The new password must differ at least with one character

2.3 Initial and Replacement Passwords

Initial passwords must be unique, complex and securely delivered. Users are automatically required to change their initial password after its first use.

2.4 Lost, Stolen, Compromised Passwords

Loss, theft or compromise of passwords shall be immediately reported to Helpdesk. The Helpdesk ensures a secure process for verifying user identity before transmitting the new password.

2.5 Password Reset Process

It’s absolutely important to identify the user which requests a reset of his password. The Helpdesk ensures a secure process for this purpose and documents all resets within the ticket tool.

2.6 Session Control and Lock-out

The following controls must be implemented:

- Automatically lock of user accounts after 5 unsuccessfully logins
- Automatically lock of user sessions after inactivity of 10 minutes

2.7 Default Vendor Password

Default passwords shall be changed before equipment is connected to our network.

2.8 Workstations / Notebooks Logical Security

- Network access is limited to computers within secure zone. Notebooks outside of our rooms must use secure VPN access.
- Administrator rights must be disabled on desktops and notebooks and it is forbidden to install own software.
- Clients, visitors etc. are not allowed to use our internal network. In this case, a Guestnet shall be provided.
- Hard discs shall be encrypted just in case of theft.

2.9 User registration and de-registration

2.9.1 Account (user) registration

Trigger point is the Human Resources department. HR and line managers must complete the access request form outlining all information systems and data for which access is required. Afterwards the complete request shall be sent to the IT Helpdesk who administer the access request.

2.9.2 User deregistration

Trigger point is the Human Resources department which must timely inform the IT Helpdesk of leaving staff. Accounts must be disabled on the day of leave.

2.10 Access Review

Normal user accounts must be reviewed within a formal process every 6 months. Privileged accounts every 3 months. Moreover, active directory must be scanned for accounts which has been inactive for more than 3 months. These accounts must be disabled.

3. Access Control to Data Center

All members of the IT department must have access to the data center in case of emergency (except the help desk). Further, the fire department must also have access to the data center in case of fire. Additionally, there might be other employees that need access to the data center on an exceptional basis.