Access Control Policy

Table of Contents

[Purpose 2](#_Toc17452500)

[Scope 2](#_Toc17452501)

[Policy 2](#_Toc17452502)

[Access control policy 2](#_Toc17452503)

[User access 2](#_Toc17452504)

[User responsibility 3](#_Toc17452505)

[Network Access 3](#_Toc17452506)

[Operating system access 3](#_Toc17452507)

[Application Access 4](#_Toc17452508)

[Monitoring System access 4](#_Toc17452509)

[Mobile Computing and Telecommuting 4](#_Toc17452510)

[References 6](#_Toc17452511)

# Purpose

The main purpose of the access control policy is to protect the security of information, assets, and client’s information and to define clearly the authorities and procedures for access control at koala corp.

# Scope

This policy applies to all employees, partners, clients, visitors and contractors who require access to koala corp. information and infrastructure systems.

# Policy

A role-based access control policy has been adopted by the koala corp. The security administrator of the koala corp. assigns one or more roles to each user

## Access control policy

Koala Corporation has adopted a kind of policy where access to password is restricted because it is the fundamental component. It will ensure a security compliance setting and secure technology platform is provided to users. It will give access to authorised account users for doing a job as set by law and agreement with valid parties. Access control policy was implemented by a reputed koala company (Hu & Kuhn, 2016). It was implemented through the identification of security access to the electronic system based on company policies. Next one is authentication of personal identification, and the last one is authorisation to the right person to use access.

## User access

In user access Koala Corporation has framed certain rules by using certain characters which can easily identify the user. It should be set in similar to the username which was known to the user and allow the user to get access quickly. Monitoring and evaluation should be done by company data administrator who is giving regular feedback about collected data. Reviewing of collected data is a critical step to ensure the ongoing process is going at the right track (Kerouh & Ziou, 2018). User access was removed after getting a personal request from a valid user and account is no longer required. User access was granted when the user clicks on direct user permission and edits user name permission and grant user name.

## User responsibility

User access control refers to the management of user account having a special privilege to access and to protect against unauthorised access. The access control of koala corp. manages the access of users to network resources and system by granting user's access to specific resources that are required for completing their job which is related to duty (Zhang, Gao, Sun & Ji, 2013). The main object behind this policy is to restrict the access to data and systems to ensure that koala corp.

## Network Access

Internet connection in a company was provided by the proper network service provider who has signed a valid agreement to be part of a network service that has all the required experience. Network enforcement was done to ensure that the network does not hamper the security position. (Zhang et al., 2019) The network should be properly configured which increases the efficiency of a network. It should fulfil the entire requirement like compatibility and justified. A network control that monitors and control an environment for a particular purpose.

## Operating system access

In koala corporation operating system access identify users through sequential access where the file is processed in order and it is most simple and common. Another method is direct access where the file is accessed not in order and it is accessed randomly. Next one is index sequential method where the index is structured to maintain a file and access can be done directly. The last one is an index access method where index allows access to files through file key and it identifies the record. Password rules are set by a data administrator who frames the rules to secure. Password should be 8 characters and it will contain both upper and lower case and also one numerical character, and special character. It should not be shared, change it if required, store it securely. Authorisation means allow the user to get access to a system and get it verified. Restriction gave to data access in the form of exchange plans catalogues, documents, journals, business process, information registers.

## Application Access

Application access to koala corp. determines the fact that whether one application can have access to the resources from another application. Application access settings are same as access controls in which they restrict access to resources but here they restrict application resources from other applications instead of restricting records and tables from users

## Monitoring System access

Koala Corporation has adopted certain procedures such as modified time, authenticated logs, audit logs, and system logs. From these data intrusion, and its attack manner can be traced and automated responses and alerts were created to detect the error. Log store all security and sensitive information and archive them for future references. It was monitored by a cybersecurity expert.

## Mobile Computing and Telecommuting

Koala corp. uses portable computers, laptops and smart phones as hosts of software that can be parameterized. Smart cards are capable of running multiple applications for travelling, making a payment or securing area access. Cellular telephones can also be used which is cap[able to make calls through cellular network technology. Koala corp. has established well-designed telecommuting programmes to enable the employees to work from home so that they can achieve a better work-life balance.

# References

Hu, V., & Kuhn, R. (2016). Access Control Policy Verification. *Computer*, *49*(12), 80-83. doi: 10.1109/mc.2016.368

Kerouh, F., & Ziou, D. (2018). Real-Time Android Application for Traffic Density Estimation. *IEEE Access*, *6*(6), 49896-49901. doi: 10.1109/access.2018.2868610

Zhang, A., Gao, J., Sun, J., & Ji, C. (2013). Declaration and Translation of Spatial Access Control Policy. *Journal Of Software*, *8*(5), 269-285. doi: 10.4304/jsw.8.5.1132-1139

Zhang, Y., Chen, X., Guo, D., Song, M., Teng, Y., & Wang, X. (2019). PCCN: Parallel Cross Convolutional Neural Network for Abnormal Network Traffic Flows Detection in Multi-class imbalanced Network Traffic Flows. *IEEE Access*, *22*(5), 1-1. doi: 10.1109/access.2019.2933165