Cyber Security Policy

Policy_2023CSP1

Human Resources

Argus Consulting

Jan 2023

Cyber Security Policy

Foreword

Our company, Argus Consulting OPC Private Limited has created this Cyber Security Policy to ensure that our data remains secure as well as our technology infrastructure. This policy outlines the various measures to ensure security to make sure that all company data and information remains protected.

Argus Consulting OPC Private Limited has developed a well-defined strategy for cyber security as well as for mitigating cyber risks to guarantee that company data is never compromised.

This policy applies to all individuals functioning under the name Argus Consulting OPC Private Limited including employees, candidates, volunteers, stakeholders, vendors, contractors irrespective of their position in the company.

Aim

- To secure Argus Consulting OPC Private Limited data and infrastructure at all costs.
- To educate individuals about the cyber security measures followed by the company.
- To define guidelines for personal use and the company
- To state disciplinary action measures in case of a policy breach.

Definitions

Confidential Data:

- Financial information of the company (classified).
- Customer data
- Vendor data
- Sales-related information
- Legal records and company contracts
- Employee information

Device Security:

- All devices must be password protected
- All devices must contain an updated anti-virus software
- Logging into company accounts must be done through secure networks only
- Security updates must be done monthly as soon as possible

Email Safety:

- Every email must be verified and checked for correct addresses and sender's name
- Clicking on suspicious links sent through emails must be avoided
- Clickbait titles and links must be avoided
- Suspicious emails can be reported to the IT department at any time.

Data Transfer Security

- Transferring sensitive company information to other devices must not be done unless absolutely necessary.
- Employees can seek the help of the IT department for transferring mass data
- Sharing of confidential information on public networks is prohibited
- Report to the IT department in case of any suspicious activity, hacking attempt, malicious activity, privacy breach, etc

Disciplinary Measures

Any individual who violates or attempts to violate Argus Consulting OPC Private Limited's Cyber Security Policy will be subjected to disciplinary action which may lead to his or her termination.

All employees will receive cyber security training annually and participation will be mandatory.

Unintentional/first-time/small-scale security breaches will be treated with a verbal warning and further training procedures. Any violation that leads to loss of company data or causes financial damage will be treated severely with legal consequences and termination.