cladtek
delivering additive solutions

Global IT Policy

Doc. No: POL-008	Revision: 4	Date: 06 Apr 2023

Cladtek Group recognises that IT is an important and indeed essential part of our business. Cladtek IT policy is designed to ensure that the systems, software, and equipment used for the purposes of the business will meet the needs of the business, add value to the business, and assure business continuity through the protection of data and system integrity, and ensure responsible and legal use of Cladtek IT.

The Use by all employees of Cladtek IT System, software, and hardware are governed by this policy. Cladtek's Employees shall follow below provision:

1. Follow company procedures with respect to IT as may be applicable from time to time
2. Use company IT System only for work purposes
3. It is prohibited to download an extensive volume of data and/or video or music streaming without a strong work value. Do understand that a wide number of people use the available systems, hence usage must be reasonable and responsible in all circumstances
4. Use the company email professionally. Remember that everything written in the email is retained
5. Consider carefully any email that will be sent to clients and/or other third-party, bearing in mind that such email represents Cladtek and may have contractual and /or legal implications
6. Do not use Cladtek email for personal matters or to express a personal opinion on any subject, and in particular, avoid making remarks of a personal nature about others in email
7. Protect the integrity of Cladtek's information by ensuring viruses are not introduced, Cladtek's data/information is not made available to any third parties without the approval of the management, and password or access control of each employee is properly managed and discreetly retained to avoid any unauthorized access
8. Only use equipment that has been authorized/approved to connect to the Cladtek network
9. Do not install or use any software that is not properly licensed
10. Do not install any unapproved or unauthorized IT Systems, software, or Hardware, without prior permission or approval from top management or Group IT Manager
11. Ensure that all data generated for or on behalf of Cladtek is stored on an electronic data system/intranet server (data is not only stored on employees' work on computers)
12. Do not intentionally or unintentionally damage or remove IT Asset facilities from hardware that has been given to the person receiving the IT Asset
13. Every hardware must use licensed antivirus software that has been standardized by the company
14. Any recording must be deleted when no longer required or when the retention period has expired
15. Any meeting (virtual/conventional) recordings must be retained only for as long as required by law or regulation, or as required by the organization’s policies and procedures

16. The use of third-party tools or software is strictly prohibited for any meetings (virtual/conventional) without permission from the Head of the Department or IT Department. If an employee wishes to use third-party tools or software (required by a customer or other government provision), they shall seek IT Department approval prior to using the application
17. Employees should be aware that some of the third-party applications may pose a security risk to the company's data and information. Therefore, the IT department will carefully evaluate any requests to use third-party applications during meetings
18. All employees are responsible for ensuring that company data and information remain secure during virtual meetings. This includes being vigilant about who has access to the meeting recordings and to any information shared during the meeting.

Cladtek encourages the responsible use of IT platforms that benefit the company through reduced costs and improved communications, such as Voice Over Internet and social media but reserves the right to refuse access to such facilities where their use is deemed excessive or incompatible with Cladtek's objectives.

Cladtek will ensure that all the data that is stored on the Cladtek network is systematically backed-up to independent hardware in multiple locations to ensure the possibility of full recovery, even in the event of a natural disaster.

It is Cladtek's policy with the respect to access to Cladtek systems that are strictly for Cladtek employees only. No one other than Cladtek employees should be granted access to Cladtek systems except with written approval granted by the CEO (Internet access with adequate security to prevent other access is excluded).

Cladtek policy with respect to IT hardware is to have an expected life of four years and then change/upgrade at the end of that period. and during that period if there is any damage caused by the user either intentionally or unintentionally, the user is obliged to replace or repair at their own expense, the company will not reimburse if there is damage and replacement of the device during the specified period.

Servers and hardware systems are designed for longer service life. Hardware should be standardized as much as possible. Hardware specifications should be updated annually to keep up with technological developments.

Cladtek undertakes to review and update this policy on a periodic basis. Cladtek also undertakes to ensure that our employees are made aware of the policy and where appropriate, provide training on and in support of the policy.

Approved by

Christopher Kamalaraj
Chief Operating Officer