Cyber Security Policy
General Data Protection Regulations
GDPR

2018

Author: Kevin Price | Cad Manager |
Implementation Date 25-May-2018
Review Date: May-2021
Endorsed by: J.E Horne (MD)

CYBER SECURITY POLICY.

POLICY BRIEF AND PURPOSE.

Laser Process Ltd Cyber Security Policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise the company's reputation. For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. Both provisions have been outlined in this policy.

SCOPE.

This policy applies to all Laser Process Ltd employees, contractors, volunteers and anyone who has permanent or temporary access to our Information Technology (IT) network, systems and hardware.

Policy elements

CONFIDENTIAL DATA

Confidential data is secret and valuable. All employees are obliged to protect this data. Common examples of confidential data are but not restricted to:

- Unpublished financial information
- Data of customers/partners/vendors
- Customer lists
- Computer Aided Design (CAD) Data

In this policy, we will give our employees instructions on how it is everybody's responsibility to avoid security breaches.

PROTECT PERSONAL AND COMPANY DEVICES

When employees use their digital devices to access company emails or accounts, they introduce security risks to our data. We instruct our employees to only use company issued computers, tablets and mobile phones to access the network. They can do this more securely if they:

- Keep all electronic devices password protected
- Install and update Anti-virus software
- Ensure electronic devices are not left exposed or unattended
- Install security updates of browsers and software monthly or as soon as updates are available
- Log onto company accounts and systems through secure and private networks only

We also instruct our employees avoid accessing internal network systems and accounts from other people's devices or lending their device to others.

When newly appointed employees receive company issued equipment they will receive instructions for:

- Installation of antivirus/anti-malware software
- Password management

They should follow instructions to protect their devices and refer to IT if they have any questions. They will also receive a copy of this policy which they will be expected to read and sign to say they have read and understand the expectations of the company in relation to GDPR, Cyber Security and IT use.

KEEP EMAILS SAFE

Emails often host scams and malicious software (e.g. worms). To avoid virus infection or data theft we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained. (e.g. "Watch this video, it's amazing")
- Be suspicious of clickbait titles (e.g. offering prizes, advice)
- Check email names and email addresses of people they received a message from to ensure they are legitimate
- Not open if unsure of validity
- Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks)

If an employee is not sure that an email they received is safe, they can refer to IT for guidance.

MANAGE PASSWORDS

Password breaches are dangerous because they can compromise the entire infrastructure of the company. Not only should passwords be secure so they won't be easily hacked, but they should also remain confidential.

For this reason, we instruct employees to:

- Have passwords with minimum of eight characters, including upper and lower case letters, numbers and symbols
- Remember your password, instead of writing it down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when finished with
- Exchange credentials (Passwords, User name) only when absolutely necessary. When exchanging them in person isn't possible, employees should prefer the phone never over email, and then only if they personally recognise the person they are talking to

Report to IT if there is any suspicion there has been a breach. New passwords will be required by all users on the company network.

TRANSFER DATA SECURELY

Transferring data introduces security risks. Employees must:

- Share confidential data over the company network, not over a public Wi-Fi or private connection
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies
- Report scams, privacy breaches and hacking attempts to IT immediately
- Send information on a need to know basis using minimum necessary information

IT must investigate promptly and resolve any issues and send a companywide alert if necessary. Hence there will be an expectation that IT will be informed by all users as soon as practicable about scams, breaches and malware so they can better protect the infrastructure.

IT is responsible for advising employees on how to detect scam emails. We actively encourage employees to discuss concerns or queries with IT.

ADDITIONAL MEASURES

To reduce the likelihood of security breaches, we also instruct out employees to:

- Lock their devices when leaving their desks
- Report stolen or damaged equipment as soon as possible to IT
- Change all account passwords at once when a device is stolen
- Report a perceived threat or possible security weakness in company systems
- Refrain from downloading suspicious, unauthorised or illegal software on their company equipment
- Avoid accessing suspicious websites

We would also expect our employees to comply with the Laser Process Ltd social media and internet usage policy.

IT should:

- Ensure firewalls, anti-virus and anti-malware software are installed on server
- Ensure Anti-virus is installed on all workstations
- Issue flash drives that are authorised for use on company network only
- Arrange for cyber security training for all employees
- Inform employees about new scam emails or viruses and ways to combat them
- Investigate security breaches thoroughly
- Follow this policy's provisions as other employees do

EMPLOYEES WORKING REMOTELY

Employees who work remotely on behalf of the company are required to adhere to the instructions in this policy. Such employees access the company's network away from the company base. Therefore they are obliged to follow all data protection standards and ensure their private network is secure.

DISCIPLINARY ACTION

It is an expectation that all Laser Process Ltd employees follow this policy at all times. Failure to do so may lead to disciplinary action.

- First time, unintentional, small security breach, such as opening an e-mail that was obviously suspicious : Laser Process Ltd reserve the right to issue a verbal warning and train the employee on security
- Intentional, repeated or large scale breaches, such as downloading unauthorised software that may infect the network. (which cause severe financial or other damage) Laser Process Ltd will employ more severe disciplinary action up to and including termination. Each incident will be examined on a case-by-case basis by the Managing Director.

Additionally, employees who are observed to disregard security instructions within this policy will face progressive discipline in the form of a written warning escalating to termination, even if their behaviour hasn't resulted in a security breach.

TAKE SECURITY SERIOUSLY

Everyone, including customers and partners, our employees and contractors, should feel that their data is safe. The only way to gain their trust is for all Laser Process Ltd employees to proactively protect the Laser Process Network, systems and databases. All employees of Laser Process Ltd can contribute to this by being vigilant and keeping cyber security at the forefront of their daily activities at work.

Backing up Data.

IDENTIFYING WHAT DATA YOU NEED TO BACK UP.

Essential data needs to be identified, i.e. the information that the business couldn't function without. (Documents, Databases, Photos, e-mails, Contacts, Customer Lists)

KEEP BACKUPS SEPARATE FROM NETWORK OR WORKSTATIONS.

All forms of backup should be restricted so they are not accessible to the general workforce. Backups must not be kept permanently connected physically or via network to the server or device holding original data. Offsite and cloud options are viable solutions. Cloud storage is where a service provider stores your data on their infrastructure, which means the data is physically separate from your original location. Laser Process Ltd company data backups are encrypted on to removable hard-drives daily. These are stored off site. The backups are also encrypted onto a Network Accessible Storage unit (NAS) that stays onsite.

The NAS has been configured to prevent potential attacks and improve security:

1. All network shares that are connected to the NAS have been disconnected.
2. Cached credentials (other than backup software) have been purged.
3. NAS Network shares have their permissions restricted to the local Admin account to the NAS only.

The 2 backup repositories are on shares \\tera01\sbs2k11 and \\tera01\Veeam in order to access either of these will immediately prompt for credentials.

With this setup it greatly reduces the risk of any automated infections from being able to attack the backup destinations ensuring that the data remains healthy in the case of a Disaster Recovery Scenario.

Backing up data should make up part of IT's everyday routine.

PROTECTION FROM MALWARE

IT to ensure all network workstations have anti-virus installed

All Laser Process staff must get authorization to download software and apps from IT. Only download from manufacture approved sites (Like Google Play and Apple app store) as these stores have greater security of their software available for download

Laser Process staff must keep all IT equipment up to date. (Patching)

Staff/User network accounts should only have access permissions to what they need

Laser Process must control how USB drives and memory cards can be used. Only authorised hardware may be used on the company network. No other data is allowed to be stored on these drives. e.g. Personal data or unauthorised software and apps

Laser Process IT must ensure firewall is on

Laser Process staff that have been issued with a mobile device, must ensure their devices are password protected and that you can track location/remotely lock/remotely erase data and retrieve data should the phone/device be lost or stolen. There is also a requirement that they keep devices and apps updated, setting to auto update is advised

Mobile device users must not connect to unknown Wi-Fi Hotspots, as they are unsecure

Laser Process staff must avoid predictable passwords by using policy rules

AVOID PHISHING ATTACKS

In a typical phishing attack, scammers send fake emails to thousands of people asking for sensitive information, such as bank details or containing links to bad websites

IT Support (OGL) to ensure accounts are configured to reduce the impact of successful attacks (Network Permissions to be configured correctly)

Employees should know what to do with unusual requests and where to get help. If unsure, employees must ask IT for advice.

If an unusual request is made via e-mail, employees should verify identity prior to opening the e-mail

IT will train staff to recognise common phishing tactics

Report all attacks

Employees are encouraged to ask for help if they think that they might have been a victim of phishing

IT to scan for malware and passwords must be changed as soon as possible if any employee suspects a successful attack

IT to report serious data breach attacks within 72hr to Action Fraud Website

https://www.actionfraud.police.uk

Telephone 0300 123 2040

CRITICAL DATA (BACK UP)

IP-Laser Data is stored in the UK at the Microsoft Azure UK South data centre.

SBS2K11 SERVER

- Combat Data
- Combat P No
- Drawings
- Opera 3
- Public

APPS01

Sigma Doc-Dwg

BACKUPS – FIREWALLS – ANTIVIRUS

Backups are carried out daily using Symantec and VEEAM software.

Backups are made onto external hard drives, the encrypted data is then taken off site overnight on a daily basis by a member if IT. There is also a copy made on to a N.A.S Drive that is hard wired, set to automatically shut down once backup has been made

Firewall Protection Employed

Watchguard Firebox (XTM3 series)

Forcepoint Exchange monitoring

Antivirus

Kaspersky End point security 10 for Windows

WORK STATIONS

Each user account holder on the company network will have a directory created on the server SBS2K11. The drive will be mapped as 'Q' on your workstation

All Business Critical Data (BCD) must be stored in that directory to ensure backups are made on a daily basis. The directory must not be used for any other purpose. Failure to save BCD in these directories could result in disciplinary action being taken

Employee Social Media Policy

POLICY BRIEF & PURPOSE

Laser Process Ltd Social Media Company Policy provides a framework for using social media. Social media is a place where people exchange information, opinions and experiences to learn, develop and have fun. Whether employees are handling a corporate media account or using one of their own, they should remain productive during work hours. This policy provides practical advice to avoid issues that might arise by careless use of social media in the workplace

SCOPE

Laser Process Ltd expects all employees to follow this policy

POLICY ELEMENTS

"Social media" refers to a variety of online communities like blogs, social networks, chat rooms and forums. This policy covers all of them

USING PERSONAL SOCIAL MEDIA

We allow employees to access their personal accounts at work. But we do expect them to act responsibly and ensure their productivity isn't affected. Using social media excessively while at work can reduce efficiency and concentration. Whether employees are using a social media account for business or personal purposes, they may easily get sidetracked by the vast amount of available content on the internet.

We strongly advise our employees to:

- *Use their common sense*. If employees neglect their job duties to spend time on social media, reduction in their productivity will be seen and possible disciplinary action taken
- *Ensure others know that personal account or statements do not represent the views or opinions of Laser Process Ltd*. Employees should not state or imply that their personal opinions and content are authorised or endorsed by the company. We advise using a disclaimer such as "Opinions are my own" to avoid misunderstandings
- *Avoid sharing intellectual property,* like trademarks on a personal account without approval. Confidentiality policies and laws apply
- *Avoid any defamatory, offensive or derogatory content*. It may be considered as a violation of Laser Process Ltd ethics, if directed towards colleagues, clients or partners

REPRESENTING LASER PROCESS LTD

Some employees represent the company by handling corporate social media accounts or speak on the company's behalf. We expect them to act carefully and responsibly to protect the company's image and reputation. Employees should:

- Be respectful, polite and patient when engaging in conversations on the company's behalf. They should be extra careful when making declarations or promises towards customers
- Avoid speaking on matters outside their field of expertise. Everyone should be careful not to answer questions or make statements that fall under somebody else's responsibility
- Never post discriminatory, offensive or libelous content and commentary
- Correct or remove any misleading or false content as quickly as possible

DISCIPLINARY CONSEQUENCES

Laser Process Ltd reserve the right to monitor all social media postings on our network and corporate accounts.

We may have to take disciplinary action leading up to and including termination if employees do not follow this policy's guidelines. Examples of non-conformity with the employee social media policy include but are not limited to:

- Disregarding job responsibilities and deadlines to use social media
- Disclosing confidential information through personal or corporate accounts
- Directing offensive comments towards other members of the online community