RJ POWER CONNECTIONS

Information Security Policy Statement CPOL- 407

RJ Power Connections Limited is an electrical contractor, with the main core of the business focusing on the supply, installation and commissioning of electrical services and systems.

This IT security policy has been introduced to RJ Power Connections and the subsidiary businesses in order to:

- Reduce the risk of IT problems;
- Plan for problems and deal with them when they occur;
- Allow business continuity if an incident occurs;
- Protect company, client and employee data;
- Protect confidential company information safe and only accessible to those who need it;
- Meet our legal obligations under the General Data Protection Regulation and other relevant laws;
- Meet our professional obligations towards our clients and customers.

Responsibilities

- Glenn Rowatt is the director with overall responsibility for IT security strategy;
- Dave Gale (IT Support Technician) has day-to-day operational responsibility for implementing this policy;
- Connect is the IT partner organisation we use to help with our planning and support;
- Mark Hayes, HSQE Manager and Jenna Wells, HR Manager provide advice on data protection laws and best practices.

Review process

We will review this policy annually. For any queries or suggestions please contact Dave Gale, IT Support Technician, dave.gale@rjpowergroup.co.uk.

Information classification

We will only classify information which is necessary for the completion of our duties. We will also limit access to personal data to only those that need it for processing.

We classify information into different categories so that we can ensure that it is protected properly and that we allocate security resources appropriately:

- **Unclassified**. This is information that can be made public without any implications for the company, such as information that is already in the public domain;
- **Employee confidential**. This includes information such as medical records, pay and so on;
- **Company confidential**. Such as contracts, source code, business plans, passwords for critical IT systems, client contact records, accounts etc;
- **Client confidential**. This includes personally identifiable information such as name or address, passwords to client systems, client business plans, new product information, market sensitive information etc.

The deliberate or accidental disclosure of any confidential information has the potential to harm the business. This policy is designed to minimise that risk.

We do not protectively mark documents and systems. Therefore, you should assume information is confidential unless you are sure it is not and act accordingly.

Access controls

Internally, as far as possible, we operate on a ‘need to share’ rather than a ‘need to know’ basis with respect to company confidential information. This means that our bias and intention is to share information to help people action tasks relevant to their job roles.

For client information, we operate in compliance with the GDPR ‘Right to Access’. This is the right of data subjects to obtain confirmation as to whether we are processing their data, where we are processing it and for what purpose.

Further, we shall provide, upon request, a copy of their personal data, free of charge in an electronic format.

Security software

To protect our data, systems, users and customers we use several security measures, including but not limited to the following:

- Laptop and desktop anti-malware;
- Server anti-malware;
- Cloud-hosted email spam, malware and content filtering;
- Email archiving and continuity;
- Website malware and vulnerability scanning;
- Intrusion detection and prevention;
- Desktop firewall;
- Perimeter firewall.

Employees joining and leaving

When a new employee joins the company, we will add them to systems relevant to their role and undertaking of their required duties.

We will provide training to new staff and support for existing staff to implement this policy. This includes:

- An initial introduction to IT security as part of their new starter induction, covering the risks, basic security measures, company policies and where to get help;
- Each employee will complete an E-learning module to raise awareness of GDPR;
- Training on how to use company systems and security software properly.

When people leave a project or leave the company, we will promptly revoke their access privileges to company systems.

Your responsibilities

Effective security is a team effort requiring the participation and support of all involved parties. It is your responsibility to know and follow these guidelines.

You are personally responsible for the secure handling of confidential information that is entrusted to you.

You may access, use or share confidential information only to the extent it is authorised and necessary for the proper performance of your duties.

Promptly report any theft, loss or unauthorised disclosure of protected information or any breach of this policy to Mark Hayes, HSQE Manager.

Protecting your own device(s)

It is also your responsibility to use your devices (computer, phone, tablet etc.) in a secure way. However, we will provide training and support to enable you to do so (see below). At a minimum:

- Remove software that you do not use or need from your computer;
- Update your operating system and applications regularly;
- Keep your computer firewall switched on;
- For Windows users, make sure you install anti-malware software (or use the built-in Windows Defender) and keep it up to date. For Mac users, consider getting anti-malware software;
- Store files in official company storage locations so that it is backed up properly and available in an emergency;
- Switch on whole disk encryption;
- Understand the privacy and security settings on your phone and social media accounts;

- Have separate user accounts for other people, including other family members, if they use your computer. Ideally, keep your work computer separate from any family or shared computers;
- Don't use an administrator account on your computer for everyday use;
- Make sure your computer and phone logs out automatically after 15 minutes and requires a password to log back in.

Password guidelines

- Change default passwords and PINs on computers, phones and all network devices;
- Consider using password management software;
- Don't share your password with other people or disclose it to anyone else;
- Don't write down PINs and passwords next to computers and phones;
- Use strong passwords;
- Change them regularly;
- Don't use the same password for multiple critical systems;
- Be alert to other security risks.

While technology can prevent many security incidents, your actions and habits are also important. With this in mind:

- Take time to learn about IT security and keep yourself informed. Get Safe Online is a good source for general awareness;
- Use extreme caution when opening email attachments from unknown senders or unexpected attachments from any sender;
- Be on guard against social engineering, such as attempts by outsiders to persuade you to disclose confidential information, including employee, client or company confidential information. Fraudsters and hackers can be extremely persuasive and manipulative;
- Be wary of fake websites and phishing emails. Don't click on links in emails or social media. Don't disclose passwords and other confidential information unless you are sure you are on a legitimate website;
- Use social media, including personal blogs, in a professional and responsible way, without violating company policies or disclosing confidential information;
- Take care of your computer and mobile devices when you are away from home or out of the office;
- If you leave the company, you will return any company property, transfer any company work-related files back to the company and delete all confidential information from your systems as soon as is practicable;
- Where confidential information is stored on paper, it should be kept in a secure place where unauthorised people cannot see it and shredded when no longer required.

The following activities are, in general, prohibited on company systems and while carrying out your duties for the company and may result in disciplinary action:

- Anything that contradicts our equality and diversity policy, including harassment;
- Circumventing user authentication or security of any system, network or account;
- Downloading or installing pirated software;
- Disclosure of confidential information at any time.

Backup, disaster recovery and continuity

We have systems and processes in place to protect our company information in the event of an incident, more information is available on request.

The types of incidents that we have considered include, but are not limited to:

- Severe transport disruption;
- Unable to access office because of flood, fire, civil disorder, terrorist incident etc;
- Loss of internet and / or phone connection;
- Loss or theft of critical systems.

We have taken into consideration how we would respond to IT security issues, including but not limited to:

- Malware infection detected by scanners;
- Ransomware;
- System failure;
- Attempted social engineering;
- Data loss or theft.

Under the GDPR, where a data breach is likely to result in a ‘risk for the rights and freedoms of individuals’ we must notify the customers and data controllers ‘without undue delay’. We will ensure we inform them within 72 hours.

All employees and others working for RJ Power Connections Limited are required to comply with this policy.

It is the responsibility of RJ Power Connections management and supervisory staff to ensure that this policy and its arrangements are implemented.

This policy will be reviewed annually and revised as often as may be deemed appropriate by RJ Power Connections Limited and then communicated and explained to all employees and subcontractors.

This policy is available to the public and all interested parties on request.

Signed:

Glenn Rowatt

Managing Director – RJ Power Connections Limited.

October 2019