15. Software Usage and Handling

At Toyama Controls, we provide various software and digital tools to support our employees in their work. To ensure the efficient and secure use of these resources, we have established guidelines for software usage, digital etiquette, and data security. Here are the key points to be aware of:

1. **Authorized Usage**: Company-provided software and digital tools are intended for work-related purposes only. Employees should use these resources solely for their designated roles and responsibilities within the organization. Personal use of office equipment, including software, is strictly prohibited.
2. **Proprietary and Third-Party Software**: When using proprietary software developed by Toyama Controls or third-party software, employees must adhere to the terms and conditions of their licenses and usage agreements. Any unauthorized installation, copying, modification, or distribution of software is strictly prohibited.
3. **Email and Internet Usage**: Employees are expected to use company email and internet resources responsibly and professionally. Email should be used for work-related communications and should not be used for personal or unauthorized purposes. Internet usage should be limited to business-related activities, and access to inappropriate or unauthorized websites is strictly prohibited.
4. **Digital Etiquette**: When using digital communication tools, employees are expected to maintain professionalism, respect, and courtesy. This includes using appropriate language, refraining from offensive or discriminatory content, and being mindful of cultural sensitivities. Confidentiality and privacy must be respected in all digital interactions.
5. **Data Security**: Protecting company data and information is of utmost importance. Employees must follow data security protocols, including maintaining strong passwords, not sharing login credentials, and refraining from unauthorized access or disclosure of sensitive information. Any potential security breaches or incidents should be immediately reported to the IT department.
6. **Personal Devices and Software**: The use of personal devices or software for work-related tasks may be subject to specific policies and guidelines. Employees should consult with the IT department or relevant authorities to ensure compliance with security and data protection measures.
7. **Software Updates and Maintenance**: Regularly updating software applications and promptly addressing any maintenance or technical issues is essential for maintaining system stability and security. Employees should promptly install updates and report any software-related concerns to the IT department.

Failure to comply with these guidelines may result in disciplinary actions, including verbal warnings, written warnings, suspension, or termination, depending on the severity of the violation and company policies.

We prioritize data security, professionalism, and responsible usage of software and digital resources. By following these guidelines, we can ensure the effective and secure use of technology in our work environment.