Policy #: IT.005–Acceptable Use Policy – IT Systems

Governed by: IT Administration
Approval Date: November 1, 2016 **Last Updated:** November 1, 2016
Purpose: Acceptable Use of CEO IT Systems

Acceptable Use Policy – CEO IT Systems

The Acceptable Use Policy for CEO IT Systems is designed to protect CEO, our employees, customers and other partners from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Everyone who works at CEO is responsible for the security of our IT systems and the data on them. As such, all employees must ensure they adhere to this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to their manager or IT Staff.

All data stored on CEO IT systems is the property of CEO. Users should be aware that CEO will take all possible measures to minimize the risk of vulnerability and/or breach with regard to the confidentiality of information stored on any CEO system except where required to do so by local laws.

Any information that is particularly sensitive or vulnerable is encrypted and securely stored on CEO server storage so that unauthorized access is prevented. CEO can monitor the use of its IT systems and the data on it at any time. This may include the examination of the content stored within the email and data files of any user, and examination of the access history of any users.

CEO reserves the right to regularly audit networks and systems to ensure compliance with this policy.