Acceptable Usage Policy - Nordics

Version: 1.4

Owner: GIS – Information Security

The policy is read and understood.

Place:_____ Date:_____

Name:_____ Signature:_____

Table of Contents

Revision History:

Version #	Revision Date (mm/dd/yyyy)	Description of Changes
1.0	07/06/2015	Initial Draft
1.1	11/30/2015	Updates to policy structure and statements
1.2	3/4/2016	Edited to correct/improve readability, grammar, punctuation, consistency, etc. Added functional TOC.

Document Control

Summary of Changes

Version #	Version Date (mm/dd/yyyy)	Author	Nature of Change
1.0	07/06/2015	Sabitri Chakraborty/ Priyanka Malik	Initial Draft
1.1	11/30/2015	Sabitri Chakraborty/ Priyanka Malik	Updated policy requirements according to review comments from policy rollout to KLT countries.
1.2	3/4/2016	Judy Gehrig	Edited to correct/improve readability, grammar, punctuation, consistency, etc. Added functional TOC.
1.3	12.01.2017	Kjetil Legreid	Re-written to include Nordic Exceptions
1.4	29.10.2018	Hilde Bekkelund	Added new password policy

Document Change Approvers

Name	Role	Approval Date (mm/dd/yyyy)

Document Review Plans

This document is reviewed and updated as follows:

- Annual review
- Any major organizational changes

1. Purpose

This document provides a set of governing principles to drive information security practices for safeguarding ManpowerGroup's information assets from intentional and unintentional mishandling, theft, misuse, or destruction by employees and third-party service providers. Adherence to this policy may improve information confidentiality and the integrity posture of the organization and may protect information assets / resources from insider and outsider threats.

The key purposes for establishing an acceptable usage policy are as follows:

- To establish a set of baseline controls for employees and third-party service providers for using the ManpowerGroup resources judiciously. These measures must be adopted to reduce the likelihood of information security issues like fraud, embezzlement, industrial espionage, and sabotage, errors / omissions, and systems unavailability.
- To provide guidance on the minimum appropriate behavior staff are expected to demonstrate to reduce the risk of unauthorized access, disclosure, modification, or deletion of ManpowerGroup information assets regardless of location and/or device type (company or personal, workstation, or mobile)..

2. Scope

The Acceptable Usage Policy is applicable to all ManpowerGroup employees, third parties, vendors, and contractors who access the ManpowerGroup information systems to conduct business on behalf of the ManpowerGroup.

The information systems include but are not limited to:

- Business applications
- Servers
- Databases
- Middleware
- Network devices (routers, firewalls, switches, IDS / IPS, and so on)
- Operating systems
- Emerging technologies such as mobile and collaborative platforms
- Hardcopy information in printed format
- Cloud applications

3. Definitions

The following table provides definitions of common terms and acronyms used across this policy.

Term or acronym	Description
Confidentiality	Confidentiality of information relates to the authorized access to or disclosure of information. Confidentiality is maintained by not making it available or disclosing it to unauthorized individuals, entities, or processes.
Critical system	A critical system is identified as one that stores / processes / transmits 'classified' or 'restricted' data and / or that has subjectively higher requirements of Confidentiality (C) / Integrity (I) / Availability (A) of data. Refer to the Data Classification policy for full definitions of "classified" and "restricted" data.
Keystroke logging software	The practice of using a software program or hardware device to record all keystrokes made on a computer keyboard.
Open source software	Open source software is freely available in the source code format. Users have the ability to modify open source software.
Peer to peer file sharing	Peer to peer (P2P) file sharing allows users to access media files (such as books, music, movies, and games) by using a P2P software program that searches for other connected computers on the P2P network to locate the wanted content.
Personally Identifiable Information (PII)	Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Examples of PII include, but are not limited to, full name (if not common), home address, phone, date of birth, residential address, and so on.
Phishing	The attempt to acquire sensitive information (such as usernames, passwords, and credit card details), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Sensitive Personal Information (SPI)	Information that if lost, compromised, or disclosed might result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of SPI include, but are not limited to, health records, gender, and so on.
Social engineering	A non-technical intrusion method that hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.
Vendor default user ID	The built-in user IDs provided with default passwords or factory settings in software and applications.

4. Policy Statements

The following statements administer the overall acceptable usage requirements for ManpowerGroup's systems, applications, networks, databases, and mobile phones.

4.1. Acceptable Usage Guidelines for End User Devices

4.1.1. General guidelines for end user devices

- ManpowerGroup systems and information processing devices must be used for intended and authorized purposes in fulfillment of organizational business goals.
- ManpowerGroup systems that are used to access / process ManpowerGroup's applications / data must not be used for inappropriate or illegal purposes.
- The computer network resources that are provided by ManpowerGroup must not be used for conducting the business of other companies or individuals.
- Employees must not intentionally access, create, store, or transmit material by using ManpowerGroup systems and devices that ManpowerGroup might deem to be offensive, indecent, obscene, or detrimental to its business interests.
- Employees must not allow family members or any non-employee to access ManpowerGroup's information stored on ManpowerGroup systems.

- Employees are responsible for protecting the confidentiality of information / data that is stored on or accessed by using ManpowerGroup systems.
- Classified or restricted information/data must not be downloaded to unauthorized ManpowerGroup devices.

4.1.2. ManpowerGroup data classification

- Information / data must be classified (categorized) based on how the information is used, its sensitivity to unauthorized disclosure, and requirements imposed by external agencies. Based on information confidentiality, integrity, and availability requirements, the following categories are defined for ManpowerGroup data / information. o ***Classified: - Sensitivity-Very High.*** Information that requires the highest level of protection because disclosure might harm ManpowerGroup's competitive position or might prompt substantial loss to ManpowerGroup's

business. It applies to both proprietary company data and sensitive Personal Identifiable Information (PII).

- o ***Restricted:*** **Sensitivity-High.** Sensitive information intended only for a limited audience within ManpowerGroup. This information includes information that relates to ManpowerGroup projects, technical data, R&D, and financial data. It applies to both company data and non-sensitive PII.
- o ***Public:*** **Sensitivity-Low.** Information consisting of general company information, widely available on publicly facing sources such as the external website or marketing materials.
- o ***Internal:*** **Sensitivity – Moderate.** Sensitive information intended for widespread distribution within ManpowerGroup and to anyone who with access to ManpowerGroup's computer systems.

- All data that is owned by, stored by, or transmitted by ManpowerGroup's information systems, regardless of the medium, must be labelled as feasible, in line with one of these four sensitivity classification options.

4.1.3. End user storage and portable computing devices

- All *portable computing devices* (such as laptops, notebooks, or handheld computers) must be protected from loss or theft:
  - o Employees must not "check" their ManpowerGroup laptop through airports as luggage.
  - o Employee must never leave their laptop or other portable computing devices unattended in a public place (such as restaurants, hotel lobbies, airport waiting areas).
- Vendors, partners, and suppliers must adopt reasonable safety measures to secure electronic media (for example, CDs, diskettes, and portable USB drives, SD cards and so on) that contains ManpowerGroup information.
- All users must use media that are provided by ManpowerGroup for their business use. Personal use of media that are provided by ManpowerGroup must be avoided.

- All hardcopy documents that are classified as "Restricted" or "Classified" must not be left unattended. For disposal, paper shredders must be used wherever available.
- Users must delete ManpowerGroup information from the electronic media (for example, diskettes, USB drives, rewritable CDs, SD Cards and so on) before the electronic media is made available for reuse.
- Any media that is no longer required for ManpowerGroup's business activities or is damaged must be promptly disposed unless otherwise implied by business requirements.

4.1.4. Mobile security

- Users of ManpowerGroup mobile devices must diligently protect such devices from loss and disclosure of classified and restricted information that belongs to ManpowerGroup.
- Employees are responsible for the physical security of employee-owned devices. ManpowerGroup is not responsible for theft or loss of employee-owned devices.
- Employees must not circumvent any security measures on the mobile device (for example, enabling USB debugging if it is already disabled or rooting the mobile device).
- If a mobile device that is contains ManpowerGroup's confidential information is presumed to be lost or stolen and cannot be recovered, the employee must disable and securely wipe the device remotely. (This action might require employee to notify the solution provider or device manufacturer if such actions must be executed by the solution provider or manufacturer).

4.1.5. Password security

- **Password construction.** Users must use strong passwords or passphrase. A passphrase is a password composed of a sentence or combination of words.

Because they are longer and more difficult for hackers to break, they are typically more secure than a password. If you choose a group of words or a sentiment that is meaningful to you and that only you know, it makes it even easier for you to remember and less likely to be compromised. One big difference between passphrases and strong passwords is that common dictionary words (with or without character substitutions, like substituting a “i” for the letter “!”) can be used in passphrases; common dictionary words are not allowed in passwords.

- Strong password and passphrase, have the following characteristics:

  Passphrase

  Must include:

  - At least 20 characters in length
  - Changed every 180 days

  Cannot include:

  - Your name, logon name or user ID
  - Character substitutions within your name, logon name, userID or company names/terms (e.g. replacing the letter “o” in your name with a symbol, like “@”, or attempting to use “M@nP@w*r”)
  - Word or number patterns or repeating characters that are 5 characters or longer (e.g. 12345, xxxxx)
  - Backward versions of items above (e.g. using “edcba” instead of “abcde”)

  Strong passwords

  Must include:

  - At least 10 characters in length
  - Contain at least one upper case letter
  - Contain at least one lower case letter
  - Contain at least one number
  - Contain at least one symbol or special character (e.g. @, $, &)

  Cannot include:

  - Your name, login name, or user ID

o Common company terms including names such as *Manpowergroup, Experis or RightManagement* or terms that are similar.

o Character substitutions within your name, logon name, user ID or company names/terms (e.g. replacing the letter “o” in your name with a symbol, like “@” or attempting to use “M@nP@w*r”)

o Common dictionary words, slang or jargon in any language

o Personal or fictional information including names, your role or position at work, or dates (such as your birthday)

o Word or number patterns or repeating characters that are 5 characters or longer (e.g. 12345, xxxxx)

o Backward versions of items above (e.g. using “rewop” instead of “power”)

o Items listed above but preceded or followed by a number (e.g. 1secret, secret1)

Passwords expire after 90 days at which time they will need to be changed.

Your new password must be different from your six (6) previously used passwords. After your successfully set a new password, it can be changed again after 24 hours.

- **Password protection.** Users must not share ManpowerGroup’s passwords with anyone, including system administrators and managers. If the password is shared with the IT/ system administrator, the user must immediately change the password.

4.1.6. Usage of unique user IDs

- To gain access to any ManpowerGroup computer system, users must use only the unique user IDs that are assigned to them. All user accounts must be unique and traceable to the assigned user.
- ManpowerGroup users must not share individual user IDs and passwords with other users.

4.1.7. Internet usage

- ManpowerGroup systems that are used to access/ process ManpowerGroup applications / data must not be used for inappropriate or illegal purposes. The users of ManpowerGroup's internet facilities must not engage in the following list of activities / websites.
    - Internet sites that contain pornographic material.
    - Internet sites that promote violence, intolerance, drug/alcohol abuse, criminal activity, or any other objectionable or illegal behavior.
    - Internet sites that allow or promote online gambling.
    - Downloading any material that does not serve a legitimate business purpose. This material includes (but is not limited to) pornographic materials, music, and video files.
    - Posting internal, restricted, or classified ManpowerGroup information on public sites
- Social media accounts (in ManpowerGroup's name (personal or official) must not be used to share or spread inappropriate content (for example, content irrelevant to ManpowerGroup's business, classified information, financial information, PII, and so on) or to take part in any activities that might bring ManpowerGroup into disrepute / or promote competitor advantage.
- Usage of content sharing platforms and uploading / downloading content: Users must not move or copy any internal, restricted, or classified ManpowerGroup information to any cloud-based file sharing system (for example, SharePoint, Google Drive, Dropbox, Microsoft One Drive and so on) on the internet unless these platforms are approved to be used to conduct ManpowerGroup business.

4.1.8. Electronic communications

- The electronic communications systems and facilities (such as e-mail, instant messaging, fax) must be used only for conducting business on behalf of ManpowerGroup and its clients.

- ***Personal communication technologies*** or accounts (including email services that are provided by third-parties such as Yahoo, Hotmail) must not be used for conducting business on behalf of the company.
- Users must not store or transmit any of the following on ManpowerGroup-managed resources (laptops, social networks, email, and so on) for inappropriate or illegal purposes, *such as*:
    - Sexually explicit or suggestive materials.
    - Materials that promote the harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, religious, or political beliefs. o Anything that is defamatory**,** threatening, profane, slanderous, or invasive of another person's privacy.
- Unless it is part of a job requirement as defined and approved by the company, the following activities are prohibited: o Sending bulk messages (unsolicited mail) to random addresses – sometimes referred to as "spam" messages.
    - Sending suspicious emails (phishing emails or suspicious active contents)
    - Soliciting others for activities unrelated to the Company's business or for political endorsement purposes.
    - Starting or perpetuating "chain" messages (any messages with embedded instructions to resend it and the instructions to others – including hoax virus warnings).
    - Sending messages with executable software attached.
    - Sending any information that might be considered proprietary or classified.
    - Using instant messaging services that are not provided or approved by ManpowerGroup.
- The ManpowerGroup employees and contractors must be aware of the following information security guidelines.
    - Users must report obscene emails. o Users must delete unsolicited emails without replying to them.
    - Users must never send passwords or other personal information about themselves to anyone.

While sending “ManpowerGroup-Classified” or “ManpowerGroup-Restricted” data, users must follow appropriate practices, as detailed in ***ManpowerGroup Data Classification Policy***.

4.1.9. Computer virus protection

- Users must not intentionally introduce any computer code that is designed to hinder the performance of or access to any ManpowerGroup computer system, network, or information (for example, computer viruses, worms, Trojan horses, and other malicious software).
- Anti-virus software must be installed on all information systems and devices, including gateways. To ensure its effectiveness, o Users must ensure that the anti-virus software is always actively running.
    - Users must not try to limit the effectiveness of anti-virus software deployed.
    - Users must report all virus incidents, suspicious files, or suspicious behavior to ManpowerGroup IT service desk.
    - Users must use the ManpowerGroup prescribed and approved anti-virus software on their workstations and laptops.
- Users must never open an email or instant messaging attachment from an unknown or suspicious source.
- If users receive a file that contains macros that they are unsure about, they must disable the macros.
- Users must be cautious when downloading files from the Internet.

4.1.10. Encryption

- ***Encryption.*** ManpowerGroup laptops, desktops, mobile devices, and other information processing systems must have ManpowerGroup-approved encryption software installed before their use within the premises. Additionally, the laptops, desktops, and other ManpowerGroup systems must be password protected and have up-to-date anti-virus software installed.

- ManpowerGroup desktop computers are generally accepted as having a lower risk of being stolen and as such most do not need to have whole disk encryption. However whole disk encryption must be enabled for the following types of ManpowerGroup desktop computers:
    - Desktop computers, due to business, geographic, or technical reasons, need to permanently store ManpowerGroup classified or restricted information locally on the computer hard disks (as opposed to a secure ManpowerGroup network server).
    - Desktop computers, due to business, geographic, or technical reasons, need to permanently host ManpowerGroup information systems (for example, MS Access, Excel) that process ManpowerGroup classified or restricted information locally on the computer hard disks (as opposed to a secure ManpowerGroup network server).
    - Desktop computers, which are located in unrestricted areas, open to the public (for example: reception desks and so on).
    - Desktop computers owned by ManpowerGroup, in third-party facilities.

4.2. Applications and Software Usage

- Only ManpowerGroup approved and licensed software must be installed on computers that belong to the company. Users must not install any software that is not owned, licensed, or supported by ManpowerGroup on computers owned by ManpowerGroup.
- Some of the examples of such unsupported software include:
    - Games, utilities, and customized screen-saver programs. These programs might change systems settings and configurations that could cause the supplied business applications to malfunction.
    - Any software that is designed to allow the computer to participate in a *"*peerto-peer*"* file sharing mode (such as Napster, Morpheus, Kazaa) that is commonly used for sharing/downloading music and video files.
    - Instant Messaging (IM) facilities that are not supplied by the company. The communication channels that are used by such facilities are not protected or controlled.

- If ManpowerGroup employees want to use open source software for official purposes, they must obtain appropriate business approvals *and* approval from the Information Security Manager/ IT department.
- ManpowerGroup employees and third parties must install the latest software updates and versions available to keep the ManpowerGroup software and applications recent and up-to-date. If standard patch-management systems prompt users to install such updates, then users must accept and install these updates.

4.3. Security Incidents

- All information security incidents or violations of security policies must be reported immediately to their local IT Help Desk or immediate supervisor. Suspicious incidents or behaviors include the following (but are not limited to):
    - Compromise of ManpowerGroup classified / restricted data to unintended parties / competitors / public at large.
    - Unauthorized access to the information system.
    - Unwanted disruption or deliberate DoS (Denial of Service). o Virus, worm, and Trojan horse detection.
    - Theft of information, data, or assets.
    - Errors resulting from negligent operations or incorrect business data or incorrect processing. o Confidentiality breaches. o Non-conformity to legal and regulatory requirements.
    - Attempts to gain unauthorized access to a system or its data; masquerading or spoofing as authorized users.
    - The unauthorized use of a system for the processing or storage of data by authorized / unauthorized users.
    - Changes to system hardware, firmware, or software characteristics and data without informing application owners.
- Employees must report such incidents directly to their local IT Help Desk or immediate supervisor.

4.4. Security Awareness Training

- ManpowerGroup users must undergo security awareness training and read the Acceptable Usage Policy, at least on an annual basis.
- ManpowerGroup users must undergo role-based security awareness training (for example, system administrators) on a periodic basis.
- ManpowerGroup users must complete additional security training when they are rolled out by the ManpowerGroup security group.

End of Document