WORK ENTERTAINMENT POINT

Cyber Security Policy

Workpoint Entertainment Public Company Limited

and its affiliated companies

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

Content

	Page
1. Message from Group Chief Executive Officer	3
2. Scope of Application	4
3. Definitions	4
4. Security Policies and Measures	5
Section 1 Access Control Policy	5
Section 2 Area Security Policy	8
Section 3 Data Backup Policy	9
Section 4 Policy for Managing the Use of Computer Programs	10
Section 5 Policy for Making Program Changes	11
Section 6 Communication Policy	12
Section 7 Computer-related Routine Work Policy	13
Section 8 Data Classification and Ownership Policy	13
Section 9 Personal Data Protection Policy	14
5.Contact and Inquiries	15

1. Message from Group Chief Executive Officer

To: All stakeholders

As Workpoint Entertainment Public Company Limited and its subsidiaries (hereinafter referred to as the "Company") are committed to establishing and developing the organization's information technology systems to ensure its security and support its confidentiality, integrity and availability of information.

Therefore, the Company has established this Cyber Security Policy with the intention to manage, determine its direction and support cyber security management, as well as build confidence in its electronic processing activities, to ensure that it is safe and consistent with the relevant cyber security measures, including the related laws and other requirements.

On behalf of the Board of Directors and executives, we sincerely hope that this Policy and measures will be comprehensively complied with by all related individuals and units.

Mr. Phanich Sodsee

Group Chief Executive Officer

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

2. Scope of Application

This Policy will be applied to Workpoint Entertainment Public Company Limited and its affiliated companies, including its directors, executives, employees and third-party service providers, who are authorized to access information at each level of security.

3. Definitions

The **"Company,"** refers to Workpoint Entertainment Public Company Limited and its affiliated companies and shall include individuals or units assigned to work on behalf of the Company, individuals or units who are authorized to act on behalf of the Company, and individuals or units who are assigned by those with authority to act on behalf of the Company.

"Directors," refers to those appointed to determine the Company's direction, strategy, and business operations.

"Executive," refers to an individual acting on behalf of, or an individual assigned to act on behalf of the executive, which herein includes supervisors who have been appointed to work in a position that is authorized for issuing orders, assigning work, directing or managing, the performance of the Company's employees.

"Employee," refers to an individual who agrees to work for the Company and receive remunerations for their work, which in this case includes employees who have passed the probationary period, probationary employees, temporary employees, employees with special contracts or employees engaged on a monthly or daily basis.

"Authorized third parties," refers to individuals who are not directors, executives or employees, nor receiving any direct remunerations from the Company, who are permitted to access information.

"Stakeholders," refers to shareholders, directors, executives, employees, creditors, customers, business partners, competitors, communities and society.

"Information," hereinafter referred to as "data," refers to news, facts, data in any form, or processed data in any event or activities.

"System administrator," refers to the network and computer system manager, the Information System Management Manager or other employees assigned by supervisors to be responsible for maintaining computers and computer networks, with access to computer network programs to manage computer network databases, and/or have been assigned responsibility for the development, revision, and maintaining information systems and various programs, that are used in the Company or a unit that is assigned with the duties and responsibility for directly maintaining computers and computer networks or information systems.

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

4. Security Policies and Measures

The Security Policies and Measures are currently classified into 9 sections as follows:

Section 1

Access Control Policy

Objective: To prevent damage from any unauthorized access to the system.

1. General Requirements

1.1 Access rights are based on the principle of allowing the Least Privilege.

1.2 Access to data is based on a need-to-know basis and the specified level of confidentiality.

1.3 Requesting access rights must be requested and recorded in writing every time. It requires that no access is allowed before approval is granted. The approver must not be the same person as the requester.

1.4 Requesting privileged access such as an Administrator, Super User, etc., must be approved by an executive at the CAO level (Chief Administrative Officer) or by the person with authority who oversees such privileges.

1.5 Requesting rights in an emergency or temporary manner must be accompanied and recorded with the reasons and necessity, including the period for expiration of the exercise of such rights. Such rights must be revoked immediately after the said period has elapsed.

1.6 Access rights of external agencies and various service providers must specify the end period and a maximum access right of not more than 1 year. New access permission must be granted on a year-to-year basis.

1.7 Those with the right to approve access include the data and/or work system owner. The IT Department is also responsible to advise on the correct right allocation procedures.

1.8 Access to data must be conducted through a secure authentication method, whereby historical access such as User Name and Password can also be verified.

1.9 Regular reviews of access rights should be conducted at least twice a year.

1.10 Access rights are required to be immediately terminated when the need for use ends or there has been a change of work duties or a contract has been terminated.

1.11 Rights to enter specific work units should be verified at least twice a year.

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

2. Access to the Network

2.1 Establish a clear segregation of network systems that separates high-priority information systems from general-purpose network systems.

2.2 Users are required to verify their identity each time they access the network system and services.

2.3 Remote access to the network must be conducted through a secure protocol such as SSH, etc. and can be allowed to access the network designated for remote use only. Such examples include designating a dedicated network zone or registering a Mac Address, etc.

2.4 Establish a remote access time limit by disconnecting the access every 5 minutes when not in use (Inactive Session).

2.5 Establish measures to prevent the installation of unauthorized programs, such as;

2.5.1 Prior to accessing the Company's network system, personal computers or laptops must be installed with anti-virus programs and vulnerability patches onto the device's operating system and web browser.

2.5.2 Users are required to update the operating system and programs with patches and/or HotFixes regularly, which can be downloaded from the product owner's website to resolve any vulnerability.

2.5.3 In transmitting computer data via email, it must first be checked for viruses by an anti-virus program before each data transmission.

2.5.4 Users must only install software provided by the Company. If the user desires to install software other than the one provided by the Company, they must first notify the IT Department to conduct safety inspections prior to installation.

2.6 The host computer system and network logs, user logging, and record of the details of the intrusion prevention system, such as Login-Logout logs, logs of login attempts, usage of the command line, logs of the firewall, must always be recorded to enable verification. Such record logs must be stored and maintained for at least 3 months.

3. Remote Connectivity and Access (VPN)

3.1 To ensure secure connections, remote users are required to connect through a VPN.

3.2 A time limit must be established for VPN usage, and the connection should be terminated when not in use.

3.3 Computers that are to be used to connect remotely should be protected against viruses and kept up to date with security patches.

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

4. Policies and Procedures for Managing System User IDs

4.1 Policies and procedures for creating user IDs and passwords.

4.1.1 In the process of creating a Standard User, the administrator must refer to the actual employee's information sourced from the Human Resources Department only.

4.1.2 In the process of creating an Administrator, approval must be requested jointly from the IT Manager as well as the Chief Administrative Officer.

4.2 Policies and procedures for changing passwords.

4.2.1 In the process of changing the password of a Standard User, the change can be made by the user themselves through the system provided by the system administrator and the password must comply with the password setting policy.

4.2.2 In the process of resetting a new password for Standard Users, the user is required to notify the system administrator of the need to reset the password via email. Thereafter, the administrator will then initiate a new password reset. In this regard, the user must change this password through the system provided by the system administrator before accessing the system or network, and the password must comply with the password setting policy.

4.2.3 In the process of changing the password of an Administrator, approval must be requested jointly from the IT Manager as well as the Chief Administrative Officer and the password must comply with the password policy requirements.

4.2.4 In the process of resetting a new password for an Administrator, approval must be requested jointly from the IT Manager as well as the Chief Administrative Officer and the password must comply with the password policy requirements.

5. Policies and Procedures for Deleting or Suspending User IDs

5.1 In the process of deleting a Standard User, the system administrator is required to refer to the employee's information provided by the Human Resources Department only, in which the names of the resigning employee will be according to the resignation effective date.

5.2 In the process of deleting an Administrator, approval must be requested jointly from the IT Manager and Chief Administrative Officer.

5.3 The system administrator can consider suspending the user IDs of Standard Users, if the following occurs:

5.3.1 The user enters the wrong password more than 3 times.

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

5.3.2 It is determined that the user can potentially cause damage to the system or database or information within the Company. In this regard, the administrator can request approval to suspend the user ID from the IT Manager and Chief Administrative Officer.

5.4 It is prohibited to use default user accounts and passwords or default information provided by the manufacturer.

5.5 Password setting requirements are as follows:

5.5.1 The password must be at least 8 characters long.

5.5.2 Passwords must contain uppercase and lowercase letters, numbers and special characters.

5.5.3 The system will force the user to change their password immediately upon first use.

5.5.4 The system forbids the user to set a new password that is the same as the last 3 times.

Section 2

Area Security Policy

Objective: To prevent damage from unauthorized access into the area, including natural disasters and accidents.

1. General Requirements

1.1 Install a personal identification system to manage access to the Data Center room.

1.2 Install protective equipment and maintain the environment appropriately, such as fire protection systems, electrical failure protection systems, water leak prevention systems, temperature and humidity control, CCTV and identity verification systems to control access, etc.

1.3 Display floor plans that clearly show fire escapes.

1.4 Conduct emergency drills and check the readiness of related equipment, such as corridor lighting, as well as the use of equipment and buttons to spray various fire extinguishing agents, etc.

2. Data Center Security

2.1 Store key computer equipment such as servers, network equipment, etc., in the Computer Center or restricted area, and the right to access the Computer Center must only be limited to individuals with related duties.

2.2 Post guidelines at the Computer Center to ensure that all relevant personnel are informed accordingly.

2.3 Crucial computer equipment must be placed in the server cabinet which should also be locked at all times.

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

2.4 In the event that an individual who does not have regular related duties needs to enter the Computer Center, it must be approved by the respective Operations Manager and be assigned with an Operations Support officer to supervise the individual at all times.

2.5 Establish a system for keeping records of access to the Computer Center. Such records must contain details regarding the individual, as well as the time of entering and exiting the Center.

2.6 Clearly segregate space in the Computer Center into dedicated zones, such as the Network Zone, the Server Zone, the Facility Zone, etc., in order to limit access to the area according to the duties and responsibilities of the Computer Center officer.

Section 3

Data Security Policy

Objective: To define procedures for backup and system recovery. This is in order to enable computer and network administrators to perform backups and restorations in a correct manner, when necessary.

1. General Requirements

1.1 Conduct regular backups of data and comply with the Company's data backup policy.

1.2 Establish a record of the backup system and always check the backup items.

1.3 In the event that a problem is encountered during the data backup process to the point where it cannot be completed, conduct troubleshooting and summarize the results of the issues and report the incident to the supervisor of the IT Department.

1.4 Assign the computer administrator to determine the type and duration of data backup as appropriate, as well as specify the media used to store data. In this regard, there are two types of backup formats: full backups and incremental backups.

1.5 Encrypt key data during the backup process (Encrypted Backup). The computer administrator must initiate encryption of crucial backup data by using appropriate encryption technology to prevent exposure of the backups.

2. Backup Procedures

2.1 Computer and network administrators must perform separate backups of each type of data. according to the stipulated frequency:

Items	Data to be Backed Up	Back Up Frequency
Web Server	Host, File Project	Daily
Database	BAK, VMDK	Daily

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

Firewall, Switch	Configuration value	Daily, before and after changes
Other system servers	Host	Daily

2.2 Computer administrators must manually verify the backup results to ensure that the backup according to details in the above table are completely correct.

3. Procedures for System Recovery

3.1 The system administrator is required to follow the procedures specified in the emergency response plan according to each incident.

3.2 Report problems and results when recovery has been completed to the Head of IT Department and the Chief Administrative Officer so that further coordination can be conducted with users.

3.3 Prepare reports of problems and log system data immediately when errors occur.

Section 4

Policy for Managing the Use of Computer Programs

Objective: To ensure that users are fully aware of their duties and responsibilities in using computer programs, as well as understand the correct use of copyrighted programs and strictly follow the established guidelines. Additionally, it is also intended to ensure that the use of computer programs is secure and consistent with computer-related offenses and relevant laws.

1. General Requirements

1.1 All related users have the responsibility for managing the use of computer programs, as well as allocating the use of computer programs within the Company according to the specified usage rights.

1.2 Related personnel are responsible for the installation and upgrade of computer programs for the Company's users.

1.3 Related personnel are responsible for removing and revoking the right to use computer programs immediately when the Company and/or work unit notifies them of any removal and/or transfer of computer program usage rights.

1.4 Computer programs must be used similar to a reasonable person would use their own property, and not use it illegally or violate the law against other parties which may cause damage to the Company.

1.5 Programs installed on the Company's computers must consist of programs for which the copyright has been legally purchased. Therefore, users are prohibited from copying illegally obtained programs and installing on the Company's computer, modifying or distributing it for others to use.

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

1.6 Users are prohibited from copying, selling or distributing pirated programs or unauthorized workflows, especially if it is capable of being used as a tool to commit crimes.

1.7 It is strictly prohibited to install illegal computer programs for use on the Company's computers. In the case that the user introduces any computer program other than the programs provided by the Company onto the computer system, regardless of whether it is a licensed software or freeware, the user will be solely responsible for any damage that may occur.

1.8 The user will be required to request the installation, cancellation of use, transfer, or return of computers, and computer programs to the authorized personnel for consideration and approval. The IT administrator will be responsible for carrying out operations as approved in each case.

Section 5

Policy for Making Program Changes

Objective: To establish guidelines for changing and modifying programs to ensure that it will be conducted in a safe and standardized manner.

1. General Requirements

1.1 Prior permission must be requested before changing a program.

1.2 The request must be sent via email or through the specified program modification request form.

1.3 A written consent must be given by the System Manager of the particular system.

1.4 When changes have been completed, it should be first tested on the QAS equipment. After receiving approval from the System Manager, it can then be subjected to actual work on the production platform.

2. Procedures for Program Maintenance

2.1 When it is deemed necessary to update or make changes to any settings, the system administrator must notify and obtain consent from the System Manager, users and relevant department heads.

2.2 When the update or change of settings has been completed, the system administrator must notify the System Manager and users and require that each user check the usage immediately.

2.3 Should a problem occur, the use of the program must be stopped and the update process or setting change be repeated.

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

Section 6

Communication Policy

Objective: To establish measures for the Company's internet and email usage. Users are required to pay close attention and be aware of issues arising from the use of the internet and emails. Users must establish a full understanding of the regulations which the network administrator has put in place. Additionally, they are also required to not violate any rights that may cause problems, or disrespect the regulations that have been laid down and must strictly follow the advice of the network administrator. This is to ensure that the use of the internet and email can be conducted in a safe and efficient manner.

1. Guidelines

1.1 Internet and email user accounts must be directly related to the employees' information as recorded at the HR Department and must only be an account created by the system administrator. For external users, permission must be obtained from the IT Supervisor or an authorized person.

1.2 The Company's internet and email systems are not to be used for personal or commercial gains, access inappropriate websites or information that may cause damage to the Company.

1.3 Internet and email users should use polite language according to the accepted customs and must be responsible for their own information that is stored on their personal computers, servers or information that is sent through the network.

1.4 Users must absolutely not allow others to use their accounts. Should a problem occur, such as copyright infringement or illegal data collection, the user account owner will be wholly responsible.

1.5 Users are urged to apply caution when downloading programs from the internet and emails. Downloading program updates must be conducted without infringing on any copyrights. Users are also urged not to download large files, but if necessary, they can do so outside of working hours.

1.6 In using the discussion board, users must not disclose the Company's confidential information, offer opinions or use provocative or slanderous language that may cause damage to the Company's reputation or break relationships with other company personnel.

1.7 In the use of emails, users must not falsify the sender's account name.

1.8 The Company's email system must not be used to disseminate information, text, images, or any content that might be deemed contrary to morality, national security, law or affecting the Company's operations, as well as causing a disturbance to other users, including the Company's service recipients

1.9 Users are required to log out after finishing using the email system.

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

Section 7

Computer-related Routine Work Policy

Objective: To establish standards for routine computer work that must be conducted on a regular basis, and used to manage problems that may occur and cause damage to users or the Company, in terms of data safety or its property.

1. Guidelines

1.1 Always prepare a checklist and organize emergency backup plan drills for every system on a regular basis.

1.2 When a problem occurs, the response procedures should be in strict accordance with the established emergency backup plan.

1.3 Establish an operator's checklist of the system, in terms of software, operating system, firmware and hardware equipment.

1.4 Conduct regular reviews of the Logging Alert records at least twice a day.

1.5 Manage inspection reports or surveys of various systems and report it to their respective supervisors.

1.6 Reports of abnormalities must be immediately made to the supervisor.

Section 8

Data Classification and Ownership Policy

Objective: To establish standards for the classification of data, to separate confidential and public information and ensure that they are clearly segregated, in terms of storage and data maintenance, including specifying the data owner so that they have the required authorization to proceed accordingly with the file or folder.

1. Guidelines

1.1 Establish data confidentiality and protect data privacy and rights.

1.2 Establish data accuracy and integrity, as well as maintain data security from inappropriate modification or destruction, including ensuring that the information is accurate.

1.3 Establish data availability that ensures that the information can be readily accessed and used in a timely and reliable manner.

1.4 Providing a stepwise creation of file and folder addresses with the appropriate access rights.

1.5 Any changes that are to be made to the file or folder access rights must be notified to the data owner and system administrator every time a change is to be made.

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

1.6 Reviews of files and folder access rights must be conducted at least twice a year and reported to the owner of the file or folder and the supervisor of the IT Department each time they are reviewed.

Section 9

Personal Data Protection Policy

Objective: To establish standards for personal data protection as specified in the Personal Data Protection Act and protect the personal information of the Company's stakeholders, customers, employees, competitors, product/service suppliers, and business partners, to ensure that they will not be used illegally or without prior consent from the owner of the information.

1. Information that are to be protected includes:

1.1 Name, surname

1.2 Age

1.3 National ID number

1.4 Telephone number

1.5 Address

1.6 Email

1.7 Photo

1.8 Work history

2. Sensitive personal information includes:

2.1 Nationality

2.2 Religion

2.3 Race

2.4 Opinions that appear on social media platforms

2.5 Religious beliefs

2.6 Sexual preference

2.7 Criminal history

2.8 Health information

2.9 Information on union affiliation

2.10 Genetic information

2.11 Biological data

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th

3. Guidelines

3.1 Establish appropriate security measures according to the minimum standards set by the work unit.

3.2 Establish procedures for the deletion of personal data files that are no longer in use.

3.3 Establish encryption for both personal and protected data, as well as sensitive personal information.

3.4 Require each work unit to assess risks and determine the level of importance of data files that must be protected.

3.5 In the collection of customers' information or third parties, it is necessary to seek permission to use the information from such persons as well as specify the effective start/end dates of the usage.

5. Contact and Inquiries

Should you require additional information, or need to make suggestions, or file complaints, regarding this information system security policy and measures, the Company can be contacted through the complaint channel on the website the following channels:

Address: 99 Moo 2, Bang Phun Sub-district, Mueang Pathum Thani District, Pathum Thani

Telephone: 02-833-2291

Email: ict@workpoint.co.th

บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน) 99 หมู่ 2 ตำบลบางพูน อำเภอเมืองปทุมธานี จังหวัดปทุมธานี 12000 โทร. 0-2833-2000 แฟ็กซ์: 0-2833-2998-9
WORKPOINT ENTERTAINMENT PUBLIC COMPANY LIMITED 99 MOO 2 BANGPOON, MUANG PATHUMTHANI, PATHUMTHANI 12000 Tel. 0-2833-2000 Fax : 0-2833-2998-9
www.workpoint.co.th