ADvTECH Group
Policy Document

POLICY NAME	**ACCEPTABLE USAGE POLICY**
POLICY EFFECTIVE DATE	**22 /04/2021**

1 DEFINITIONS

Unless the contrary is clearly indicated, the following words and/or phrases used in this Policy shall have the following meaning:

1.1 **"ADvTECH"** or **"We"** means ADvTECH Limited and its subsidiary companies;

1.2 **"Business Unit/Business Units**" means any of the trading divisions of ADvTECH, including Support Offices;

1.3 **"BYOD"** Bring your own Device is the practice of allowing the employees of an organisation to use their own computers, smartphones, or other devices for work purposes;

1.4 **"Cable Lock"** means a security cable with a lock which is used to attach Portable IT Equipment to a fixture;

1.5 **"Channels"** means any communication channel or system including but not limited to social media applications whether or not these are hosted or owned by ADvTECH;

1.6 **"Communication"** means the transfer of information, including a message or any part of a message whether in the form of speech, music or other sounds; data; text; visual images, whether animated or not; signals; or radio frequency spectrum; or in any other form or in any combination of forms, that is transmitted in whole or in part by means of a telecommunication system (including but not limited to a fixed telephone line, cell phone device, computer and Internet based Communication Facilities), this includes communication of any of the above or similar on any social media channel;

1.7 **“Communication Networks”** means any network system, or series of electronic communication facilities or radio, optical or other electromagnetic apparatus or any similar technical system used for the purpose of electronic communication, whether such electronic communication is subject to re-arrangement or not, composition or other processes by any means during their transmission or emission or reception;

1.8 **“Contractor”** means any natural (who is not an employee) or juristic person who provides products and or services of any nature to ADvTECH, pursuant to a binding agreement with ADvTECH;

1.9 **“Damage”** means any physical damage to the Portable IT Equipment that is determined by the supplier to be physical damage for example the outer casing, the laptop screen, keyboard and touchpad mouse;

1.10 **"Data Protection Legislation"** means any data protection or data privacy laws applicable to ADvTECH or the Group, including but not limited to POPI, the Electronic Communications and Transactions Act 26 of 2005, the Promotion of Access to Information Act, 2 of 2000 and the Consumer Protection Act 68 of 2008;

1.11 **“Designated Areas”** means areas where visitors or occasional third parties may meet with You. This should be areas which does not allow access to secure areas where the required access controls are applied.

1.12 **“Device/s”** means any machine, mechanism or other device made for electronic communication purposes, which is personally owned or used by an identifiable living natural person, which is not limited to smart phones, tablet computing devices or notebook computers;

1.13 **“ECT Act”** means the Electronic Communications and Transactions Act 25 of 2002;

1.14 **"Deputy Information Officer"** means a person appointed by or on behalf of ADvTECH as a deputy information officer, who is required to assist with the implementation of the policy, and who will be able to assist with the compliance requirements of this policy;

1.15 **“Equipment”** means computers of all kinds, servers, routers, modems, telephones, cell phones, electronic handheld devices, facsimile machines, pagers, SMS devices, software, hardware and/or similar equipment owned by, licensed to or rented by ADvTECH. This definition excludes private cell phones and computers when used for business purposes;

1.16 **“Facilities”** means any physical location or premise that is used by ADvTECH representatives (partners, employees, third parties and contractors) to process ADvTECH owned information (or information within ADvTECH’s possession) in either electronic or physical form;

1.17 **"Group"** means every South African entity over which ADvTECH exercises control and which is considered a subsidiary company;

1.18 **"Information Assets"** means Information or record, in either electronic or paper form, that has value because its use is necessary for the execution of operations and the achievement of goals for ADvTECH. Information and information assets may be used interchangeably;

1.19 **"Information Regulator"** means the independent body established in terms of section 39 of the Protection of Personal Information Act 4 of 2013 subject to the law and the constitution;

1.20 **"Information Systems"** means any system, hardware (including devices and equipment), software or network that is used to process ADvTECH owned information (or within ADvTECH's possession) in electronic form;

1.21 **"Intercept"** means the acquisition of the contents of any Communication through use of any means to make some or all of the contents of a Communication available to a person other than the sender or recipient or intended recipient of that Communication It includes the monitoring of any such Communication by means of a Monitoring Device, viewing, examination or inspection of the contents of any Communications and the diversion of Communication from its intended destination.

1.22 **"Internet"** means a publicly accessible network or networks that use the TCP/IP Communications protocol and include several subset protocols and services such as the World Wide Web (www), Network newsgroups (NNTP), social media channels and internet relay chat (IRC), and shall in all cases include Interchange, cell phone networks or wireless areas;

1.23 **"Monitor"** means to analyse, review, listen to or record Communications by means of a Monitoring Device;

1.24 **"Monitoring Device"** means any electronic, mechanical or other instrumental device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or Record any communication as determined in the Regulation of Interception of Communications and Provision of Communication-Related Information Act no 70 0f 2002 from time to time;

1.25 **"Loss"** means the act of losing one or more of ADvTECH's Portable IT Equipment or when one or more of ADvTECH's Portable IT Equipment is taken or stolen;

1.26 **"Partner/s"** means a business partner who enters a contract with ADvTECH;

1.27 **"Person"** means an identifiable, living, natural person or identifiable existing juristic entity;

1.28 **"Personal Information"** means information that relates to an identifiable and living natural person (which includes employees, students and prospective students, parents, candidates and prospective candidates and suppliers) and where applicable, an identifiable and existing juristic person (such as a company, close corporation, or a trust). This information includes: (a) information describing a person, such as their race, gender, sex, pregnancy, marital status, national, ethnicity, colour, sexual orientation, age, health, disability, religion or beliefs, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of a person; (c) any identifying or contact details (such as a person's name, e-mail address, physical address, telephone number, location information); (d) the biometric information of the person; and (e) the personal opinions, views or preferences of (or about) a person or any communications set to or from a person;

1.29 **"Policy"** means this Acceptable Usage Policy together with any guidelines or annexes that form part of it;

1.30 **"POPI"** means the Protection of Personal Information Act, 4 of 2013;

1.31 **"Portable IT Equipment"** means laptops, a small compact portable computer, Notebooks, Netbooks, company issued cell phones, digital cameras or similar equipment, including data connectivity cards/modems, projectors and external hard drives owned by, licensed to or rented by ADvTECH;

1.32 **"Premises"** refers to any building owned or occupied by ADvTECH;

1.33 **"Processing"** means activities that involve personal information, including activities such as collecting, storing, using, disseminating, marking, restriction, erasing or destroying Personal Information;

1.34 **"Secure area"** means an area which can only be accessed by persons who are duly authorised.

1.35 **"Service Desk"** means the telephone, website, or other communication channel through which you may report any contravention of this policy, by logging an incident.

1.36 **"Student"** means a person engaged in study at an ADvTECH institution;

1.37 **"Third Party"** means any other party (organisation or person) other than ADvTECH or its partners.

1.38 **"User"** means any person who has access to or use of ADvTECH's Information Assets IT Equipment and IT resources;

1.39 **"User Identification (User-ID)"** is a logical entity used to identify a user on a software, system, website or within any generic IT environment. It is used within any IT enabled system to identify and distinguish between the users who access or use it. A user ID may also be termed as username or user identifier."

1.40 **“You"** means ADvTECH's directors, employees, contractors, agents and partners and any other third parties involved in the Processing of Personal Information and similar activities;

Although the definitions above have been capitalised, they may be referred to within this document in their normal lower-case form. Where their meaning differs from the definition, it will be explained.

2 INTRODUCTION

This Policy applies to all users who have access to and/or use of ADvTECH Group’s (“ADvTECH”) information, electronic and computing devices, IT infrastructure, and networking resources. In addition, this Policy applies to all users who have access to and/or use of ADvTECH’s Communication Facilities or Channels. It should be read in conjunction with other related ADvTECH policy(ies).

3 PURPOSE

Computer information systems, technology, networks and the systems and channels that make use of this technology are an integral and valuable part of ADvTECH’s business. ADvTECH has invested significant capital and resources to maintain these systems and networks and the integrity and operation thereof should always be protected. The purpose of this Policy is to:

3.1 inform users about the use of ADvTECH's information systems, technology and networks;

3.2 inform users on the appropriate use of any communication technology including social media channels and systems whether or not these are housed on ADvTECH Facilities and Equipment;

3.3 create rules for the use of ADvTECH's information, technologies, assets, resources and Communication Facilities and inform users in relation to these rules;

3.4 provide for the interception of communications and monitoring of communication using Facilities and Equipment or Channels;

3.5 where individuals use their own devices, sections of this policy will not apply but you must apply common sense and good judgement. Where there is ADvTECH data or software on the device security and data controls will be applied by ADvTECH;

3.6 clarify responsibility and provide the appropriate action when Loss or Damage to IT Equipment has occurred;

3.7 provide for clarity on how to deal with transgressions of this Policy; and

3.8 ensure and maintain the security, value and integrity of ADvTECH's Equipment and network(s) and reputation in so far as it can be impacted by electronic communication of any sort including social media.

4 SCOPE

This policy applies to:

4.1 all divisions and Business Units;

4.2 You and all users;

4.3 all information under the jurisdiction and/or ownership of ADvTECH whether located at ADvTECH or non-ADvTECH locations;

4.4 any device/IT infrastructure within ADvTECH's information processing facilities, or authorised to access ADvTECH's information processing facilities; and

4.5 all information, either new or existing and in electronic or paper form.

5 POLICY RULES

5.1 Communication, Social Media and Electronic Communication

5.1.1 Communication Facilities and Equipment at ADvTECH are primarily provided as business tools. All Communication Facilities and Equipment must be used primarily for ADvTECH's business purposes. ADvTECH does not normally block access to social media or non-business-related communication, but will do so when required and reserves the right to monitor or investigate potential abuse or violation of this policy.

5.1.2 Social media and electronic communication (hereafter social media) may be utilised while at work to conduct and further ADvTECH's business where appropriate, subject to the adherence of the provisions of this Policy and related policies governing conduct while associated with ADvTECH.

5.1.3 The personal use of social media while using ADvTECH property, resources and time is discouraged and where it impacts on productivity, may be considered as an abuse of company resources. Similarly, private, and personal use in moderation of Communication Facilities and Equipment is accepted subject to the rules detailed in this Policy. Common sense and good judgement should guide users in private usage. When using facilities for private use, it must be kept in mind that the purpose of the provision of such facilities is for business effectiveness and thus communications may be accessed by the business.

5.1.4 The transmission of confidential company information, customer data, trade secrets, and any other material covered by existing company secrecy policies and procedures and relevant national and international legislation, by means of any Communication Facility, to any unauthorised persons both internally and externally is prohibited.

5.1.5 ADvTECH has the same expectations of employee and contractor conduct and behavioural standards in a virtual world or when using any form of electronic communication as is expected in other areas of life. ADvTECH explicitly reserves its rights to defend its reputation and that of its stakeholders in all spheres of your life. This includes but is not limited to comments and statements made in social media.

5.1.6 ADvTECH has a zero-tolerance approach against any prejudice or discrimination.

5.1.7 All representatives (employed or contracted) are expected to apply the same values, ethics, policies, expectations, guidelines based on sound judgement, respectfulness and common sense that would conform with ADvTECH's own values and ethics when interacting with colleagues, parents, students and prospective students, learners, candidates and prospective candidates', alumni, shareholders, suppliers, members of the public, media and other constituencies of ADvTECH ("stakeholders"). For the avoidance of doubt, this principle requires you to conduct yourself online as you are required to do in person.

5.1.8 Any Record or other content that is generated using the Communication Facilities and Equipment will remain the property of ADvTECH and should always be treated as though others may later view them.

5.2 Log-on Policies

5.2.1 User responsibilities for their User-IDs

To ensure that system logs reflect the true identities of users, and to preserve the accountability and integrity of access controls, the sharing of personal User-IDs and passwords or the use of User-IDs belonging to another user is strictly forbidden. In addition generic and service accounts are not authorised to access data.

5.2.2 Password Use

All users must be authenticated through an authentication mechanism, the minimum being a unique, personal, and secret password.

5.2.3 User Access Authorisation

Access to ADvTECH's information systems must be authorised by the application owner.

5.2.4 Assignment of Access Privileges

Group IT – infrastructure and application owners must specify user access privileges based on the principles of "need to know" and "need to use" and balance functionality against security requirements when approving access to information systems.

5.2.5 Review of User Access Privileges

Group IT – infrastructure and application owners must review all user access privileges to information systems on at least an annual basis and/or after any significant changes taking place within ADvTECH.

5.2.6 Securing Unattended Workstations

No computer equipment, device, or terminal may be left logged on while unattended. Users must lock or log off when stepping away from their desks. This principle applies when users work remotely, regardless of the remote location.

5.3 Secure Remote Working

5.3.1 Authorisation for Remote Working

5.3.1.1 All users wishing to access the ADVTECH network from a remote location must obtain formal approval from their line management before such access is granted.

5.3.1.2 Requests for remote access must be made using a standard Remote Access request form or online process, and are only for valid business reasons where:

5.3.1.2.1 Users are away from the office for considerable periods of time and require access to perform necessary job functions;

5.3.1.2.2 Users are on standby and require access to the corporate network for after-hours information systems support;

5.3.1.2.3 Users demonstrate ADvTECH products and need off-site access to the network for the purposes of the demonstration;

5.3.1.2.4 Users need access to process and approve business requests; and

5.3.1.2.5 Other reasons that are deemed by a user's line manager to be valid business reasons.

5.3.2 Connections for Remote Working

Remote access to any external sources while connected to the ADvTECH network is strictly prohibited.

5.4 Backing up of Information Stored on Company Devices

5.4.1 Users are responsible to back up data they are working with.

5.4.2 The backing up of any ADvTECH information on personal devices is strictly forbidden unless ADvTECH security standards for such devices have been applied.

5.4.3 Users must ensure that all company information, inclusive of personal information that is stored on their workstations or other computing devices is saved onto Office 365 through the use of OneDrive or SharePoint Online.

5.4.4 Users must manage their data in accordance with the Data Retention and Data Classification Policies.

5.5 Storage of Company Information

5.5.1 Storing company information on mobile devices (such as, but not limited to, laptops, storage devices, tablet PCs and smart phones), home computers, and unauthorised third party cloud providers (e.g. Dropbox) is strictly prohibited, unless ADvTECH security standards for such devices have been applied.

5.6 Physical security

5.6.1 Entry Authorisation

5.6.1.1 Access by employees, contractors, third parties including visitors to designated areas must be approved by the relevant managers or authorised personnel before such access is granted. The relevant managers remain accountable to ensure compliance with the access procedures of each Campus or Business Unit.

5.6.2 Visitor Access Controls

5.6.2.1 Visitor access to ADVTECH secure areas may be granted for specific authorised purposes (e.g. business meetings, maintenance & repairs, deliveries, etc.) only once the identity of the visitor has been cleared by the staff member they are there to see.

5.6.2.2 All visitors must sign the visitor's register and specify the name of the staff member being visited.

5.6.3 Escorting Visitors

5.6.3.1 Visitors granted access to secure areas must always be supervised.

5.6.4 Reporting lost or stolen Access Cards

5.6.4.1 Physical access cards that have been lost or stolen (or are suspected of being lost or stolen) must be reported in line with the relevant campus/site rules pertaining to access cards as well as to the person's immediate line manager.

5.6.5 Forgotten Identity Badges/Access Cards

5.6.5.1 Users who have forgotten their identification badges/access cards and wish to access ADVTECH premises will be considered "Visitors".

5.6.6 Obtaining New or Replacement Identity Badges/Access cards

5.6.6.1 New cards will be created with the minimum required identity information (e.g. Name, Surname and Identity number) based on the rules of the specific campus or Business Unit pertaining to the issuing of new Access cards.

5.7 Removal of Company Property

5.7.1 Issued hardware (e.g. laptop) may be taken home by the person to whom it has been issued.

5.7.2 An Asset Taken Out Form (Annexure B hereto) must be completed where a user wants to remove hardware from ADvTECH which has not been issued to them.

5.7.3 Spot checks may be done by the business to ensure compliance.

5.8 Clean Desks

5.8.1 All information classified as Highly Confidential or Confidential, whether in paper form or electronic form (e.g. external hard drives etc.) must be securely filed when the information is not in use.

5.8.2 Highly Confidential and Confidential information must be locked in areas where stringent access controls are in place.

5.8.3 Periodic clean desk reviews may be conducted by line management and users that are identified as not complying may be subjected to a disciplinary enquiry.

5.8.4 The provisions of this clause also applies where users work remotely.

5.9 Returning company information and devices

5.9.1 All ADvTECH information, regardless of what it is stored on or where it is kept, must be handed over to the Business Unit or Department head (or duly appointed representative) when an employee, contractor or third party's employment comes to an end, or when they stop providing services to ADVTECH. Failure to do so could result in the ADvTECH taking the necessary steps against such an individual, which may include the laying of criminal charges for theft.

5.10 Malicious Software and Virus Protection

5.10.1 To protect ADVTECH's information and operations from any damage or disruption from viruses, malware or any other malicious programs, users must comply with the following:

5.10.1.1 Respond immediately to any viruses, malware or malicious programs detected on their workstation or computing device by informing the Group IT located in their office or campus. The IT Department must assist in identifying and removing the malicious code and repairing any damage that resulted from the malicious code infection.

5.10.1.2 Not uninstall, deactivate, reconfigure, or attempt to circumvent the malicious code software installed on a workstation or computing device.

5.10.1.3 Take all reasonable steps to ensure that their home computers and/or mobile devices (such as, but not limited to, laptops, tablet PCs and smart phones) are suitably protected with using up-to-date anti-virus management software.

5.11 Use of ADvTECH IT Equipment and Facilities

5.11.1 ADvTECH's insurance policy only covers the costs of recovering stolen Portable IT Equipment whilst on ADvTECH's Premises.

5.11.2 The user will be held responsible for the replacement cost of the Portable IT Equipment in the event of loss or damage resulting from negligence by the user.

5.11.3 If the loss or damage to Portable IT Equipment is not because of negligence on the part of the user, the head of the business unit has the discretion to determine the appropriate action and allotment of costs.

5.11.4 Users must notify line management in the event Portable IT Equipment is Lost.

5.11.5 Immediately report to the Group IT Service Desk upon becoming aware of a lost or stolen personal device with access to ADvTECH resources. This should be done as prescribed by the Loss Control Policy. ADvTECH IT must then remotely remove applications and data from these devices.

5.11.6 Files or folders on workstations or other computing devices may only be shared by using tools provided by ADVTECH, such as One Drive or SharePoint.

5.11.7 Users must report any Portable IT Equipment damage to their IT Department.

5.11.8 Users must ensure that all Portable IT equipment is secured to the home office desk, office desk, floor or wall with a cable lock during work hours.

5.11.9 Users leaving Portable IT Equipment at work overnight must ensure that it is locked in a safe place. Only business-related information may be stored on servers and hard drives. Any files not required for business purposes may be deleted without warning at ADVTECH's discretion.

5.12 The Interception and Monitoring of Communications

5.12.1 Any personal communication sent, stored, or received via ADVTECH's communications facilities may, without further notice, be monitored, intercepted, inspected, or refused by duly appointed company representatives in the exercise of their responsibility to ensure continued optimal operation of these facilities.

5.12.2 The typical reasons for such action may include, but are not limited to:

5.12.2.1 Ensuring that ADVTECH's communications are not being used in violation of this policy;

5.12.2.2 Counteract criminal or fraudulent activities;

5.12.2.3 Protect the communications facilities from intentional and unintentional damage;

5.12.2.4 Respond to legal proceedings that call for evidence; and

5.12.2.5 Conduct investigations in connection with alleged abuse of the communications facilities.

5.12.3 ADvTECH's right to intercept any Communications shall only commence with the prior written authority of Chief Information Officer.

5.12.4 Any person who intercepts communication or has access to intercepted communications must sign a non-disclosure agreement prior to such interception and undertake not to disclose the interception process, the identity of subject and/or any related information, unless authorised to do so by due legal process or for the purposes of disciplinary or legal action.

5.12.5 Unless such disclosure is authorised by due legal process or for the purposes of disciplinary or legal action, the following information are prohibited from being shared with third parties:

5.12.5.1 Private, personal and confidential information collected through the interception of communications; and

5.12.5.2 The identity of users whose communications are or were the subject of interceptions.

5.13 Unacceptable Use

Users may not:

5.13.1 View, store or distribute any material that is sexually explicit, pornographic, racist, sexist, or derogatory of race, origin, sex, sexual orientation, age, disability, religion, or political beliefs;

5.13.2 View or access pornographic or obscene material without the prior consent of the research committee and/or the Director or Registrar of The IIE who will consider if there is an academic instructional or research reason for such assess to be permitted;

5.13.3 View, store or send messages intended to harass, intimidate, threaten, embarrass, humiliate, or degrade someone or that contain references that cause offense;

5.13.4 Misrepresent, obscure, suppress, or replace a user's identity (pretending to be someone else) on a communications system as this is strictly forbidden;

5.13.5 Send or forward spam or chain mail;

5.13.6 Share ADvTECH information using external email services such as Gmail or personal e-mail accounts provided by personal Internet Service Providers (e.g. MWEB);

5.13.7 Connect to personal Internet Service Providers (ISPs), or other third parties from ADVTECH's IT network (whether directly or through the use of a phone line), without prior written authorisation from Group IT, or as part of a remote working practice is strictly forbidden;

5.13.8 Use company e-mail facilities to send advertisements of a personal nature;

5.13.9 Use Facilities to send out bulk e-mails to multiple addresses or send any other such unsolicited bulk communications using Social Media unless authorised to do so in the ordinary course of the user's official business;

5.13.10 Remove or amend any disclaimers or signatures (e.g. email signatures) present when using ADVTECH communication facilities;

5.13.11 Download, install, store, or distribute pirated software or data, entertainment software, music, or games;

5.13.12 Download any programs or software, whether freeware, shareware, trial/demo, or utility, without prior authorisation and an ADvTECH owned license

5.13.13 Copy ADvTECH software for use on any computer other than the ADvTECH supplied desktop or laptop computer where the software license does not allow for it, without written permission;

5.13.14 Copy or grant access to ADvTECH software for distribution to independent contractors, clients or any third party without written permission;

5.13.15 Overcome the security mechanisms of the equipment or any third party security system or website;

5.13.16 Excessively download, reproduce, share, retain and/or create Records that contain music, images, sound, or video if such Record is not reasonably required for the user's official business;

5.13.17 Copy, destroy, delete, distort, remove, conceal, modify, or encrypt messages or files or other data on any company computer, network, or other communication system without the permission of an authorised individual. This includes copying to online storage like Google drive;

5.13.18 Attempt to access or access another person's computer, computer account, e-mail or voice mail messages, files or other data without their consent or the consent of an authorised individual;

5.13.19 Violate or attempt to violate any other applicable laws, regulations, or provisions, including the violation of terms governing cross-border flow;

5.13.20 Intentionally damage IT equipment;

5.13.21 Leave portable devices in plain sight in a vehicle;

5.13.22 Leave portable devices at work overnight unless locked in a safe place or secured with authorised personnel.

5.13.23 Unless authorised by Group IT, develop or maintain a web server on the company network or create and use their own SQL server;

5.13.24 Use any intellectual property (logos, images, iconography, and names) of ADvTECH or any of its stakeholders on any personal Social Media to promote any unauthorised product, cause, political party, or candidate or to imply in any manner endorsement of and individual or product or service or cause by ADvTECH. The name of ADvTECH or the business unit where the individual works can only be used to describe the place of work of that individual where this is required to make sense of the Social Media profile or channel; and

5.13.25 Post anything which belongs to anybody else without their written permission. Users are required to adhere to standard intellectual property and academic integrity conventions by providing links to source material whenever possible.

Included in this Policy are some practical guidelines to be followed when using Facilities and Equipment. Please refer to Annexure A.

6 REPORTING PROCEDURES

6.1 If you have been involved in or become aware of any violation of this Policy by another person, it is your responsibility to report it to the ADvTECH Deputy Information Officer or the Service Desk as soon as possible.

6.2 To the extent possible and practical, ADvTECH will endeavour to maintain the confidentiality and anonymity of the report. If you fear reprisal, you should express this concern at the time of the report. In such circumstances your identity will be kept confidential.

6.3 ADvTECH will investigate each reported violation and will take the appropriate action. All users have a responsibility to assist and cooperate in any investigation conducted by ADvTECH or by the Information Regulator.

6.4 Retaliation, retribution, or harassment against anyone who in good faith reports a violation of this Policy is strictly prohibited and, where applicable, constitutes grounds for disciplinary action, including dismissal.

6.5 In circumstances where you wish to report a violation anonymously, you should contact the Hotline. The Hotline telephone number and website are secure and administered by the ADvTECH Group Internal Audit department in conjunction with Group IT.

6.6 Any person or employee who intentionally discloses false information knowing that the information is false with the intention to cause harm to the affected party would be guilty of an offence and be subjected to disciplinary proceedings.

6.7 Users working remotely must ensure that loss or damage to mobile or remote working equipment, as well as any ADVTECH information on such equipment, is reported promptly to Group IT.

6.8 Any loss of personal information whether suspected or actual, must be reported as per the ADVTECH Group Information Privacy Policy.

7 CONSEQUENCES OF NON-COMPLIANCE

7.1 Although your line manager is responsible for the implementation and monitoring of the adherence to this Policy, you are responsible for your own actions. Consequences of violations of this Policy are serious and may expose ADvTECH to litigation and fines, result in harm to its reputation as well as its competitive position. Violation of certain provisions of applicable Data Protection Legislation amounts to a criminal offence, which may result in imprisonment of the individuals involved.

7.2 Non-compliance to this Policy may result in a User's email privileges or access to any Facilities or Equipment or Channels being suspended pending the outcome of a disciplinary hearing.

7.3 Anyone who is found to have consciously engaged in unlawful Processing activities or to be negligent in exercising his or her managerial responsibilities in preventing a violation of this policy will be subject to disciplinary measures and may in certain cases face dismissal and/or the immediate termination of the business relationship between the parties.

7.4 In any case of doubt regarding any of the information contained in this Policy or whether any content or information considered for posting on social media may violate the terms of this policy, employees and contractors are urged to liaise with their relevant managers or people in authority.

8 OWNERSHIP AND RESPONSIBLE PERSONS

8.1 Users are personally responsible to abide by the rules created in this Policy and may be subject to audits without notice.

8.2 Group IT, located at support office, in conjunction with the IT departments of the various subsidiary and/or associated companies are jointly responsible for:

8.2.1 The technical issues related to the access and use of ADvTECH's Communication Facilities and Equipment;

8.2.2 Assisting ADvTECH's management in intercepting communications and investigating breach of the provisions of this Policy;

8.2.3 Ensuring that all outgoing email messages contain ADvTECH's official email legal notice;

8.2.4 Scanning, filtering, and blocking all electronic communications for damaging code such as viruses;

8.2.5 The maintenance and management of this Policy; and

8.2.6 Group HR, located at support office, in conjunction with the HR departments of the various subsidiary and/or associate companies are jointly responsible for bringing this Policy to the reasonable attention and access of all users and ensuring that every user agrees in writing to ADvTECH's right to intercept any communications.

9 REVIEW OF POLICY

9.1 This Policy shall be revised upon the occurrence of any one or more of the following:

9.1.1 The anniversary of the effective date;

9.1.2 Amendments to Acts pertinent to Communications, Security or Privacy;

9.1.3 Drafting of further Policy(s) that have a direct bearing on the obligations contained in this Policy;

9.1.4 Revision of any Policy(s) that have a direct bearing on the obligations contained in this Policy;

9.1.5 Other statutory amendments or legislative requirements considered just cause for review;

9.1.6 Reasons pertaining to the operational requirements; or

9.1.7 Ad-hoc revisions.

9.2 Outcomes of the review and updates shall be made available to the you at the first available opportunity after the review and shall be distributed by the person designated from time to time.

10 LEGISLATION COMPLIED WITH IN THIS POLICY

10.1 The Electronic Communications and Transactions Act 25 off 2002;

10.2 The Regulation of Interception of Communications and Provision of Communication Related Information Act 20 of 2002; and

10.2.1 Protection of Personal Information Act 4 of 2013

Annexure A

BEST PRACTICE GUIDELINES

1 Usage of Portable Equipment:

Below are best practice guidelines which describe how to carefully treat Portable Equipment. This includes:

1.1 shutdown laptops when not in use to avoid overheating especially before placing it in a laptop bag;

1.2 hard drive and display should be set to turn off after a period of time when laptops are not in use;

1.3 use a hard surface under your laptop as often as possible; as a soft surface can block the airflow vents and cause overheating;

1.4 before packing your laptop in a bag, unplug all accessories;

1.5 do not to leave your laptop on the floor. It can easily get damaged;

1.6 Users must take all reasonable steps to preclude onlookers from viewing any company information.

1.7 Similarly, you should take care when communicating via mobile phones.

1.8 Use a good quality bag that is designed to carry Portable IT Equipment; and

1.9 never check your laptop in as luggage when travelling on an airplane.

2 Usage of Electronic and Social Media

2.1 **Always identify yourself** – whenever you are posting content related to ADvTECH identify yourself from the outset as an employee, contractor or third party acting on behalf of ADvTECH. It is never acceptable to use an alias, misrepresent yourself nor to hide your affiliation to ADvTECH.

2.2 **Personal Views** – whenever you are posting personal views relating to ADvTECH make it clear that the views expressed are your views, using a statement as follows: “The views expressed here are my own and are not necessarily those of the ADvTECH Group or any of its Brands”.

2.3 **Think twice before posting** – Privacy does not exist in Social Media. You are personally responsible for the information you are entrusted with and the content you post on Social Media. Consider what could happen if a post becomes widely known and how it could affect ADvTECH, its stakeholders and you.

2.4 **Understand that online activity is permanent** – Everything posted on Social Media will probably stay online for a very long time. It is almost impossible to completely remove information from Social Media since there is no way of knowing where it may have been reposted and/or shared. There is no way to ensure that a post was seen and shared, even if it is later edited, removed, or deleted.

2.5 **Recognise that you are entering into a social environment** – Engaging in Social Media is like participating in a social event such as a meeting, a conference, or a party. The same good manners apply: introduce yourself, be courteous, don't pretend to be someone else, don't intrude in or interrupt the conversations of others. Don't lie. Behave as you would in the real world – consistent with the image you want to portray in the office.

2.6 **Strive for accuracy** – Provide informed, well-supported opinions and if necessary, cite sources. Although Social Media is a more casual form of communication, it is still important to be factual. Always write in the first-person tense. Always review the content to ensure that the statements are truthful, and the grammar and spelling are correct.

2.7 **Be Respectful** – Any content posted on Social Media could encourage comment and the discussion of opposing ideas. Consider your response carefully and how they could affect ADvTECH, its stakeholders and you.

2.8 **Remember who may read your post** – ADvTECH has many stakeholders. Consider everybody who is likely to read your post before posting it to ensure that you will not alienate, harm, or provoke any stakeholder.

2.9 **Be the first to correct your own mistakes** – If you have accidentally posted something that was not appropriate or true, be the first to respond. If you need to modify a post, make it clear that you have done so.

2.10 **Keep calm** – If a debate becomes heated, be conciliatory, respectful and quote facts to diffuse the situation and correct misrepresentations. If you feel you are unable to respond professionally then refer the matter to another team member.

2.11 **Be Careful** – There are real risks when working on the internet, communication channels or social platforms. Other points to always keep in mind is:

2.11.1 exercise caution when downloading files or information from the Internet.

2.11.2 do not place undue reliance on the correctness of such information, unless verified from an independent, reliable source.

2.11.3 You are reminded that ADVTECH's communications facilities (whether e-mail, Internet, voice, or fax) are not automatically protected against disclosure to unauthorised individuals. Therefore:

2.11.4 Sensitive company information may only be transmitted via the Internet (e.g., when sending an e-mail message to a recipient outside of ADVTECH) when suitable measures have been employed to ensure the confidentiality of such information;

2.11.5 When scanning and emailing sensitive company information users must ensure that they remove the document from the scanner as soon as the procedure is completed.

2.11.6 When communicating via a voice network (e.g. telephone), users must verify the identity of the individual and ensure that the individual on the line is authorised to receive company sensitive information.

2.11.7 Note that sensitive company information is any information defined as Confidential or Highly Confidential in the ADVTECH Data Classification Policy.

2.12 **Protect confidential and proprietary information** – You are expected to adhere to all applicable privacy and confidentiality policies, legislation, and regulation. This includes not posting content or speculation about ADvTECH's business performance, future products, pricing decisions, unannounced financial results, predictions, legal matters, stakeholders or any other confidential or proprietary information.

2.13 **Legally Binding** – The communications sent by employees, contractors and third parties, whether electronic, paper-based, or otherwise, may be legally binding upon ADVTECH, therefore users must ensure that they do not bind ADVTECH to any undertaking or statement unless they are authorised by ADVTECH to do so.

2.14 **Distribution Lists and Social Media Channels** – have been created to facilitate communications with ADvTECH. Misuse of these constitutes a contravention of this Policy. For example, copying User for User off the Global Address List (to include the entire system address book) to be incorporated as addresses is not permitted. A user may only send and/or use distribution lists or Channels that the user is authorised to use. If a user needs to send a communication to a distribution list that the user is not entitled to send to and/or use, then the user must send the communication to ADvTECH's IT Department and request that the IT Department send the communication to the relevant distribution list.

2.15 Sending and Receiving of Communications

2.15.1 Keep communications brief and appropriately formulated;

2.15.2 Users should take care when receiving e-mails with file attachments, even if that e-mail appears to come from a known source;

2.15.3 Check communication recipients prior to sending, forwarding ore replying to messages;

2.15.4 Ensure that the subject field of any communication directly relates to the contents and purpose of the communication;

2.15.5 When forwarding or replying to communications, the contents of the original must not be altered. If the contents of a communication need to be change, then all changes must be clearly marked as such;

2.15.6 Spam is becoming increasingly problematic, therefore

2.15.6.1 Users must refrain from publishing their communication address on websites or newsgroups;

2.15.6.2 or following unsubscribe" links in spam communications;

2.15.6.3 opening spam communications. If a spam communication is opened, this signals that your e-mail address is active and more spam will follow;

2.15.6.4 visiting any of the websites linked in spam e-mails; and

2.15.6.5 replying to any spammers, requesting they stop sending e-mail. Replying will only serve to confirm your e-mail address is active and more spam will follow;

2.15.7 All spam messages must be forwarded to themarshal@advtech.co.za. This message and the domain from where it originated can then be filtered from the server in future.

2.16 If a user is out of the office for more than one day, they should activate the "Out of Office" function. This informs the sender of an email of the user's absence. The "Out of Office" message should include both the period of absence and an alternative contact person.

2.17 You may not send communications on behalf of an alias (such as helpdesk@advtech.co.za) or on behalf of another user (such as a manager) unless you have the written permission of your manager, which has been forwarded to the Chief Information Officer and Head of Human Resources.

2.18 All mailboxes have been limited in size per user. It is the responsibility of each user to maintain a limited mailbox size. The Sent items, Deleted items and Inbox folders should be checked regularly and mail that is no longer necessary deleted.

2.19 The size of Outgoing and Incoming messages, including attachments has been limited to 34 Megabytes at ADvTECH. Every user should take note that external service providers may have set smaller limits for messages received/sent by them; and

2.20 Where possible, large documents with attachments should be compressed using an industry standard compression tool, such as Windows Compressed Files (a feature in the Windows Operating System) and sent using functionalists such as Mimecast.

Annexure B

Asset Take Out Form