IT User Policy

Introduction

The aim of this policy is to ensure that Everest's IT facilities can be used safely, lawfully and equitably. These rules are in place to protect employees, suppliers and associates of Everest. Inappropriate use exposes Everest to risks including virus attacks, compromise of systems, brand damage and legal issues. Accordingly, such inappropriate use is likely to result in disciplinary or equivalent action against anyone infringing this policy.

Scope

This policy applies to anyone using the Everest IT Facilities (hardware, software, data, network access, third party services, online services and telephony). This policy also applies to privately-owned hardware when accessing Everest's IT services remotely.

Equality Analysis

Everest is committed to equality of opportunity and the promotion of diversity for all employees of the company. Equality analysis is a process which examines how the impact of the policy has been considered on the diverse characteristics and needs of everyone it affects. This policy has been reviewed and no negative impact of equality has been identified. The policy is reviewed by the Executive Team on a yearly basis.

Responsibility

It is the responsibility of all users of Everest's IT services to read and understand this policy. This policy may be updated from time to time to comply with company and legal requirements.

This IT User Policy is intended to provide a framework for such use of Everest's IT resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

Data Protection

Every employee shall comply with the requirements of the Data Protection Act 2018 ("the Act") (which incorporates the General Data Protection Regulation) concerning personal data in their use of IT facilities. In particular:

1) Personal data, and devices holding data, must be kept securely. Devices must be kept in locked cupboards when not in use and must be password protected in accordance with this policy;
2) Personal data held on authorised company devices may only be held and used in accordance with the company's data policies;
3) Personal data must not be copied to or stored on USB or other external drives/media;
4) Personal data must not be shared or transmitted outside of the business via or through use of IT facilities unless to the data subject themselves (or their properly-authorised agent) or with the express permission of the company's Data Protection Officer.

For further details, please see the company's Data Protection and Data Security Policies. Any data that is held on an individual is called "Data Subject".

Security of IT Equipment

All employees responsible for Everest IT equipment must take adequate precautions to ensure that the physical environment is secure in order to deter illegal access to equipment and/or theft. The level of the security should be appropriate to the type and location of the equipment. Laptops, for example, must NOT be left in vehicles overnight.

Passwords

Network passwords are set to change every 40 days. When choosing a password, think about what is obvious and choose something else. A good password should be at least 8 characters long and include Upper Case, lower case, a number and at least one wildcard (*, @, !).

When using documents with customer details in, always password protect them. If emailing these kind of documents, never send the password in the same email as the attachment – send it in a following email.

Email Usage

Email should be used for business reasons only. Address emails only to those people who NEED to see/respond to the email. Do not copy in people arbitrarily. You must:

1) Archive email over 6 months' old;
2) Save attachments to the shared drive and delete them from your email box;
3) Clear your Sent box periodically;
4) Remember to clear your Deleted Files folder.

Consent to intercept and disclose data

The use of Everest's IT services is subject always to the condition that Users consent to the examination of any data stored in computers, computer systems and any electronic devices and to the examining, monitoring and interception of data, communications or contents of computers by Everest for lawful purposes whenever it is deemed necessary, together with the authority to pass such data legally to third parties as reasonably required.

This work is normally carried out by IT Services or the Legal Department on behalf of Everest in order to meet the operational and security needs of the company and any related investigatory activities.

Risk Assessment and Management

Risk assessment and management is seen as a vital component of Information Security. To determine the appropriate level of security measures to be applied to information systems, it is important that a process of risk assessment is carried out for each system to identify the probability and impact of security failures. This will be done by IT Services with assistance from the appropriate Head of Department.

Return of Equipment to Everest Head Office

Both Users and their Managers are jointly and severally responsible for ensuring the return of equipment to Everest Head Office if no longer in use. The equipment should be in good, clean and working condition. If not, a charge may be applied to the User and/or Manager who sent the return. Failure to return the equipment may also result in a charge.

For leavers, Managers (including TDM's) are responsible for ensuring the return of equipment to Everest Head Office in a good, clean and working condition. If not, a charge may be applied to the Manager/TDM who sent the return. Failure to return the equipment may also result in a charge.

Use of mobile devices

Everest will only provide a mobile device (phone/tablet/dongle) if there is an essential business need specific to the individual role. Applications must be approved by the relevant Line Manager or Budget holder.

Everest will offer a limited range of handsets/tablets/dongles with the appropriate mobile tariff, determined based on the needs of the individual. Mobile equipment issued by Everest has to be used primarily for business use. Inland Revenue guidance does permit an employee that has been issued with a business mobile device to make calls or use it for personal reasons, but only when private use is "not significant".

Everest's mobile devices will be locked down, using Maas360, to restrict what can and cannot be downloaded onto the device. Users will not be permitted to download Apps from the Apple app store. If an app is required for business reasons, the user must email the IT Service Desk to seek approval and the app will be made available from within the Maas360 app store.

Use of, or subscription to, premium and/or interactive mobile services using an Everest mobile device is strictly prohibited. This includes (but is not limited to) the downloading or forwarding of ring tones, videos and mobile-TV. Failure to comply with this may result in disciplinarily action being taken against an employee, as well as all charges associated with such use being passed on to the User.

Everest does not permit the transfer of the Everest SIM card from the supplied mobile device to a personal device. This may incur substantial costs for incorrect tariff usage and Everest will seek full recompense for any additional charges incurred due to this action. It may also cause serious security breaches where 'data' based devices carry company confidential information.

All users must be aware that usage will be monitored on a regular basis. Employees who are allocated a mobile device will be held responsible for the device and all calls made and other charges incurred. It is therefore essential that devices must be kept secure at all times and use by anyone other than the named individual is prohibited.

The Handset/Tablet/Dongle/SIM PIN code or other security locking system should always be used. Sensitive information (e.g. personal data, passwords, or any other data that could bring Everest into disrepute should it fall into the wrong hands) should not be stored unsecured on a mobile device. Personal data should not be stored on any mobile device.

Devices that are lost or stolen must be reported immediately to Everest IT (IT.Support@everest.co.uk or 0330 33 22 500) so that the handset can be deactivated. It is strongly recommended that users keep a separate note of their handset's IMEI number as this will need to be provided to the mobile provider to deactivate the device.

Mobile devices remain the property of the company at all times and must be surrendered when an Employee leaves employment or as determined by the head of department, HR or Everest IT.

Having placed an order for a mobile device, users should be aware that this means Everest are entering into a two-year contract with the service provider. The user is therefore issued with the device for a minimum period of two years. The device is available to the user as long as they remain with the company and their role requires them to use the mobile device.

Users must not under any circumstances re-allocate mobile devices to others without first seeking authorisation from Everest IT. In the event that Everest IT authorise the reallocation of a device to another individual, all elements of the contract including phone number will also be transferred.

Requests for non-standard mobile devices and contracts purchased by the company will only be agreed where specialised mobile devices are required or as a reasonable adjustment for any Employee with specific requirements due to a disability. Approval must be sought from a Director or Head of HR.

Guidelines

DO	DO NOT
Do use a strong password and change it if you think it has been compromised	Do not give your password to anyone else
Do report any loss or suspected loss of data to the Data Protection Officer	Do not re-use your Everest password for any other account
Do be on your guard for fake emails/calls asking for confidential information	Do not open suspicious emails, documents or links
Do keep software up to date and use antivirus on all devices	Do not undermine the security of the Everest network
Do be mindful of the risks in using public WIFI or computers	Do not provide access to Everest systems through these public access points
Do ensure Everest data is stored on Everest systems only	Do not copy confidential company information without permission
Do password protect and encrypt your personally owned devices	Do not leave your phones or computers unlocked

Unacceptable Use

1) Everest’s IT network may not be used directly, or indirectly by a User for the download, creation, manipulation, transmission or storage of:
   a) Any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
   b) Unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
   c) Unsolicited “nuisance” emails;
   d) Material which is subsequently used to facilitate harassment, bullying and/or victimisation of another employee or a third party;
   e) Material which promotes discrimination on the basis of race, gender, religion, belief, disability, age or sexual orientation;

f) Material with the intent to defraud or which is likely to deceive a third party;
g) Material which advocates or promotes any unlawful act;
h) Material which infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party;
i) Material that brings Everest into disrepute;
j) Material which is defamatory to Everest, its products and services, colleagues and customers.

2) Everest's IT network must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:
a) Intentionally wasting employee effort or other Everest resources;
b) Corrupting, altering or destroying another User's data;
c) Disrupting the work of other employees or the correct functioning of the network;
d) Denying access to the network and its services to others;
e) Pursuance of commercial activities, outside of an employee's employment with Everest.

3) Any breach of industry good practice that is likely to damage the reputation of the Everest network will also be considered as unacceptable use.

4) Users shall not:
a) Introduce data-interception, password-detecting or similar software or devices to the Everest network;
b) Seek to gain unauthorised access to protected parts of the Everest network;
c) Access or try to access data where the User knows or ought to know that they have no access to;
d) Carry out any hacking activities;
e) Intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software;
f) Needlessly repeat email sending to group distribution lists which causes offence or wastes others time in reading such emails

Breach of policy

Any breach of this IT User Policy will be considered a matter for disciplinary or equivalent action and a User's access rights may be revoked pending investigation.

Where appropriate, Everest will disclose information to law enforcement agencies and take any legal action against a User for breach of this policy, including, but not limited to claiming all costs, fees and disbursements (included but not limited to legal fees) connected therewith.