

# Policies



# DRESS CODE

## What are the organization's expectations?

While you will be able to use your discretion while dressing for work, below are a few guidelines that you are expected to comply with.



### General expectations

- All associates are expected to be clean and well-groomed
- Clothes should always be clean, neat and tidy
- Shirts and t-shirts should be tucked in for men
- Always need to wear ID card



### Monday to Thursday (Smart casuals)

#### Gentlemen

- Formal trousers
- Collared tee shirts
- Closed formal shoes

#### Ladies

- Two-piece or full-length dresses
- Salwar-kameez or saree



### Friday

#### Gentlemen

- Jeans
- Collared tee shirts
- Sports Shoes

#### Ladies

- Jeans
- Formal shirts, and trousers or skirts



# DRESS CODE



## Business formals for important meetings, events and forums

### Gentlemen

- Formal shirts
- Formal trousers
- Closed formal shoes

### Ladies

- Two-piece or full-length dresses
- Salwar-kameez or saree

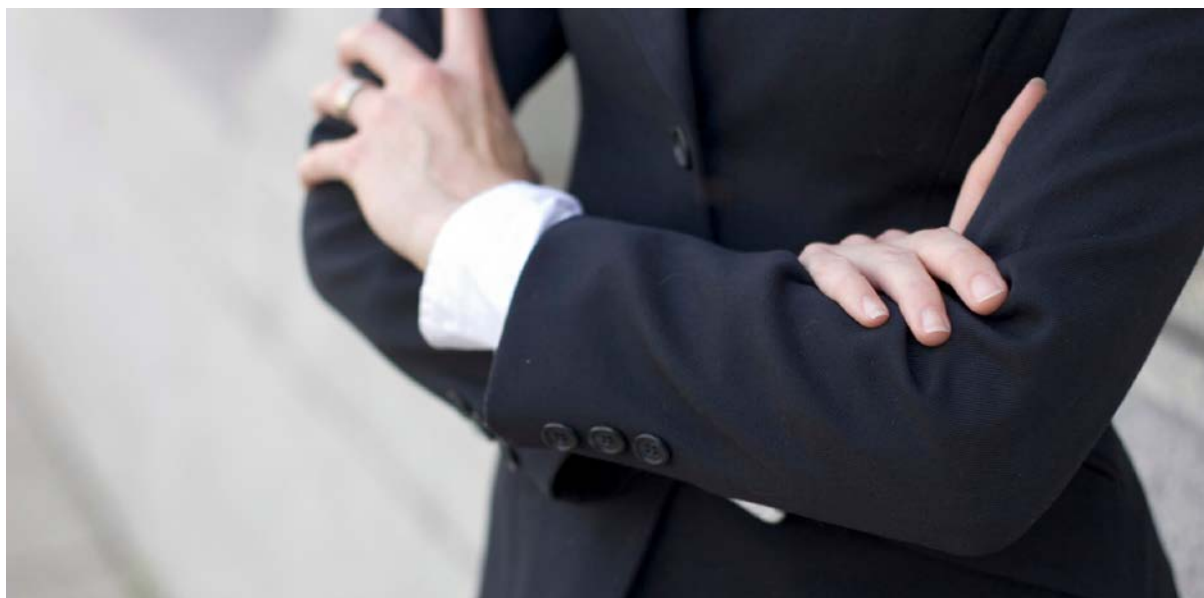
HR personal will let you know on prior for respective dress code on any festive occasion conducted in office for a traditional wear.



## Inappropriate attire

- Rubber slippers, torn denim or other trousers, shorts, casual skirts, round-neck tee-shirts, gym clothes and any attire bearing offensive messages or prints are inappropriate in any situation.
- Leather slippers, shoes without socks are considered appropriate footwear for ladies but not for gentlemen.
- Kurta-pyjama, sherwani, dhoti, etc. are not recommended

**We expect you all to follow the same to make AMBC proud**





# LEAVE POLICIES



## Permission

Two hours of permission is allowed throughout a month in adjustable divisions. There will be an additional two hours just in case of emergency with reasonable explanation. If permission exceeds more than two hours, then it will be calculated as half day leave.



## Flexible timings

30mins of flexible time from actual working hours and the employees should complete 9 hours of work. Late login for more than half an hour, it will be deducted from the 2 hours of permission every month even if 9 hours are completed.



## Sick leave

Backup resource should be mentioned while applying leave.



## Earned leave

5 working days' prior notice with the reason to get approval from Reporting Manager. Absence without intimation or without approval will be treated as leave without pay.



## Compensatory Off Policy

Compensatory off will be availed by employees if they work only on National Holidays



# LEAVE APPLYING PROCESS



## Process for Planned Leaves (For all Client representing employees)

- All employees need to inform about leave prior 5 business days via mail to [Senior Management Executive & Vice President](#)
- In the mail you need to mention your leave days and the resource who will be respective backup. If there is no backup, what are your plans with respect to daily tasks?
- Senior Management Executive will take care of delivering information to the client and get an approval
- After getting approval you need to apply leave in HR Portal



## Process for Planned Leaves (For all Non-Client representing employees)

- All employees need to inform about leave prior 5 business days via mail to [Senior Management Executive](#)
- In the mail you need to mention your leave days and the resource who will be respective backup. If there is no backup, what are your plans with respect to daily tasks?
- After approval you need to apply leave in HR Portal



## Process for Emergency / Sick Leaves (For all Employees)

- All employees need to inform via Mail / Phone / Text to [Senior Management Executive](#)
- Senior Management Executive will take care of necessary action accordingly for approval
- After returning you need to apply leave in HR Portal

### NOTE

You need to apply the leave within 5 days from the day you take the leave in HR Portal. Any leave which is not applied through above process or not applied in HR Portal will be considered as LOP.



# IT SECURITY (UNSUSPICIOUS EMAIL)

If you receive any unsuspicious email from any third party sites. Kindly forward phishing email to IT Security Team



## How to recognize phishing email from third party

**Unfamiliar sender identity**

Thu 7/3/2014 2:56 AM  
Mail Administrator <Secure-mail@ust.hk>  
HKUST Mail Upgrade

**Downloading unknown attachment can be dangerous**

You forwarded this message on 7/16/2014 11:23 AM.  
Message: HKUST-CentralAuthenticationService.htm (4 KB)

**Threatening user that their account will be deleted if they do not response**

We are working hard to fight phishing/spamming. We have upgraded our platform to a more better and Secure one. You are required to download the attachment, Sign in twice for you to enjoy this platform.

**Failure to validate your account may result to loss of important information in your mailbox or cause limited access to it**

We are sincerely sorry for any inconvenience this might cause you; we tend to serve

**No real person's name included and no mention of a phone number to call or person to contact**

Helpdesk  
2014

**Hover the mouse cursor over the link to Check where the link actually points. In this case It points to "malicious-website"**

Visit us on <https://www.ambconline.com>

<http://malicious-website/secure-mail@ust.hk>

<http://malicious-website/secure-mail@ust.hk>

Ctrl+Click to follow link





# IT SECURITY (UNSUSPICIOUS EMAIL)

To report a phishing scam, **forward the phishing email as an attachment to [security@ambconline.com](mailto:security@ambconline.com)**.

## ★ Reporting a phishing scam in Microsoft Outlook (Desktop client)

- Select the suspicious email in Outlook.
- Press **Control-Alt-F**. This will open a draft email message with the suspicious email as an attachment.
- Add [security@ambconline.com](mailto:security@ambconline.com) in the **To:** field of the draft email message.
- Send the email.

## ★ Reporting a phishing scam in Microsoft Outlook Online (Office 365)

- Select **New** to compose a new message.
- In the upper right-hand corner of the new message, click the icon to compose the message in its own window.
- Drag the suspicious email into the body of the new message. This will add the suspicious email as an attachment.
- Add [security@ambconline.com](mailto:security@ambconline.com) in the **To:** field of the draft email message.
- Send the email.

# IT SUPPORT EMAIL

Any additional software that is needed for work, must be approved by the management and downloaded/installed by the IT Department only





# INFORMATION SECURITY MANAGEMENT SYSTEM POLICY



We strive to achieve total information security by...

- Following good practices to protect the organization's information assets from internal or external / deliberate or accidental information security threats
- Aligning information security management with the organization's strategic risk management context
- Setting information security objectives, and establishing a direction and principles for action
- Establishing criteria for risk evaluation and risk acceptance
- Controlling access to information assets (including networks) based on business and security requirements
- Protecting information and physical media in transit
- Protecting information associated with the interconnection of business information systems
- Putting safeguards in information sharing
- Observing clear desk policy for papers and removable storage media
- Observing clear screen policy for information processing facilities
- Implementing appropriate security measures in mobile computing and communications





# INFORMATION SECURITY MANAGEMENT SYSTEM POLICY



We strive to achieve total information security by...

- Establishing rules for the development of software and systems and applying these rules to developments within the organization
- Ensuring protection of the organization's assets that are accessible by suppliers
- Prohibiting the use of unauthorized software and complying with laws on intellectual property rights
- Protecting organizational data and safeguarding privacy
- Taking back-up copies of information, software, and system images and testing them regularly
- Retaining records for sufficient period before disposing them carefully
- Taking disciplinary actions and discourage misuse of information services by personnel
- Complying with applicable requirements related to information security, including the requirements spelt out in the ISO/IEC 27001:2013 standard
- Reviewing the effectiveness of ISMS at regular intervals, and
- Continually improving our ISMS.



# MOBILE PHONE

- All the employees are advised to put your mobile phones in **SILENT MODE**.
- Use company-issued phones for business purpose only.
- Employees are **NOT ALLOWED TO USE** mobile phone camera's or microphone inside the office premises
- Employees can make their brief personal calls away from the work space during **THEIR BREAK TIME** or **IN CASE OF EMERGENCY**.
- Watching videos, playing games or using social media applications during work hours are **STRICTLY PROHIBITED**.



# Thank You

