Information Security Awareness Training
for Nestlé Account Staff

2016
Contents

• Training Objective
• Why is Information Security Important to Us
• Information Handling
• How is Information Secured
• Nestlé GLOBE Policies, Standards and Guidelines
• HPE User Access Management
• Password Management
• Security Incident Management and Reporting
• Account Security Officer Role
• Information Security Daily Practice
• Useful Links
Training Objective

This training is part of account administered information security awareness program and is MANDATORY for all HPE personnel working on the Nestlé account. The content will help account staff to:

- Understand all the applicable HPE and Nestlé security policies
- Learn how to apply those policies within the service delivery
- Educate them about their commonly shared IT security responsibilities
Information Security

Why is it important to us?

– HPE is protected by YOU

– Every Nestlé account staff (permanent & contingent) is responsible for protecting HPE and client Information Assets and should be aware of all Information Security requirements

– People are the first line of defense against various threats and are the most important assets of HPE

– Legal and regulatory requirements – EU Data Privacy (GDPR), Data Protection Act of Switzerland, ISO27001, etc.

– Nestlé holds sensitive customer data which must be protected
Information Handling
Security Guidelines for Handling Information Assets

– All HPE employees share the **responsibility for protecting** HPE physical and/or electronic information from unauthorized access.

– The responsibilities and obligations for handling both HPE and Nestlé confidential/sensitive information are documented in the existing **contractual documentation** per project.
  – HPE has similar agreements with our other customers, therefore **sharing or exposing other HPE customer confidential or sensitive information to Nestlé is strictly forbidden**.

– Sharing/access permission to information is based on job-related function and need-to-know.
  – Avoid sharing the data unless strictly necessary for business purposes and unless you have management endorsement to share the specific information in question.

– Instead of forwarding electronic copies, you can store the information in the established collaboration platform (e.g. SharePoint) and provide reference to it.

– Use password protected (encrypted) archives to share highly sensitive information.

– Host Skype meetings yourself and encourage contractors/third parties to join over the phone. If needed, you can also leverage the HPE **MyRoom** functionality for presentation and collaboration.

– Follow the standard HPE labeling guidelines for handling and managing information assets.
  – Just because information (such as an electronic file or hardcopy document) is unlabeled, you must not presume that the information is public domain; rather, all information at HPE is to be presumed as **confidential**.

– More detailed information on this topic can be found in the HPE-Nestlé Information Handling Security Guidelines document.
How is information secured?

Enterprise Security Policies and Standards

Aligned to the HPE framework is the HPE Enterprise Security Information Security Policy framework housed within the Enterprise Security Information System (ESIS) portal. Enterprise Security Policies and Standards (ESPS) is the HPE ES repository that contains information security best practices and expertise gathered from around the globe. It also provides the baseline to which all infrastructures in the service delivery environment must be designed, built and maintained in order to provide the quality of secure information asset protection our clients expect and deserve.

HPE Standards of Business Conduct (SBC) are the overarching guides for all behaviors, processes, and policies within HPE.

Policies are a high-level commitment taken to protect assets and information - in all forms. They are statements of specific, high-level security needs and often include pointers to standards.

Standards specify the actions that must be taken to achieve the objectives of the security policy.

Control Procedures or Specifications are the detailed implementation procedures that must be executed to ensure that a standard is effectively and consistently performed – how to carry out the policies.

Global Compliance Management System (GCMS) contains compliance events, third party audit activities, recurring manual (self-assessment) checks, which provide assurance that operations are implemented and functioning as intended.
Nestlé GLOBE Policies, Standards and Guidelines
Customer policy overview

– HPE is responsible for keeping the Design, Infrastructure and Service provided by us complaint to the Nestlé security policies and standards, as mandated by the current contracts.

– Some relevant Nestlé GLOBE Security Policies, Standards and Guidelines:
  ❖ GD-19.400 Internet Service Use in Nestlé
  ❖ GD-19.401 Remote Access Services and Solutions
  ❖ GD-19.402 Payment Card Industry Standard
  ❖ GD-19.403 User Management
  ❖ GD-19.404 Password Management
  ❖ GD-19.408 Operating System Security
  ❖ GD-19.409 Network Security
  ❖ GD-19.414 Reporting Information Security Breach Incidents

– Links to above documents available here.

– If there are no relevant policies for a particular technology area provided by Nestlé, HPE’s ESIS policies should be consulted. The same is valid for missing technical procedures, standards and best practices.
HPE User Access Management
Process for provisioning HPE users on Nestlé account

– HPE UAM administrator is the first point of contact for new team members in order to obtain the needed access level to the customer environment.

– Several prerequisites must be met before access is provisioned:
  – Requestor has passed all mandatory trainings for their role (including this one).
  – Requestor have read and signed off on the Nestlé Confidentiality agreement.
  – Requestor obtained all needed approvals (both internal and client side).

– Requester should contact the UAM administrator with an email containing their desired access level (role).

– HPE UAM administrator will respond with the relevant access request requirements and steps to complete the request.
  – Please read and follow all instructions provided by the UAM administrator.
  – Provide all required information and relevant approvals for the requested access level.
  – All accounts should be personal accounts and sharing of account credentials is not permitted.

– SAP HANA specific guidelines and detailed process description can be found in the HPE SAP HANA Access Management Guide.
Password Management
Guidelines how to properly manage personal & generic account passwords

Your identity is yours only – learn how to protect it!

Passwords are like toothbrush or bubblegum:
➢ Never share with anyone
➢ Change periodically

– As per Nestlé polices for generic account management, all passwords for generic (system or non-human) accounts must be “vaulted” and access to them restricted.
  – Password exchange for those must always be done over approved secure channels

– Do not hardcode or store your password in plain text
  – KeePass Password Safe (1.04 or higher) an “approved” password vaulting tool according to both HPE and Nestlé security policies.

– You can use the built-in KeePass Password Generator tool to generate Nestlé compliant passwords.

– More detailed information how to install and configure KeePass for personal use can be found in the HPE SAP HANA Access Management Guide.
Security Incidents
What are they and how to treat them?

– Incidents that affect the confidentiality, integrity and availability of Nestlé or HPE assets constitute a security incident and must be reported.

– Common threats are equipment theft, loss of data, social engineering, phishing and malware.

– It is responsibility of each employee to report a physical security (PS) or information security (IS) incidents to the Account Security Officer (ASO).

– The ASO is responsible for direct communications with the customer but will need your support for:
  – identifying the incident
  – technical inputs for the impact assessment
  – remediation and mitigation recommendations
  – providing status updates on the incident

– Events that threaten HPE/Nestlé employees or impose significant reputational, financial or operational risks are considered as critical and must be escalated to account management and CIM teams.
Security Incidents
Where to report them?

Physical Security Incidents refer to actions or events that threaten the physical security of HPE’s workforce, workplace, or assets. Examples include: acts of violence, verbal threats, thefts, and other suspicious activities or criminal acts. Report all Physical Security Incidents to Global Security Services (GSS).

IT Security Incidents pose risks to HPE which could result in unauthorized disclosure of sensitive data, destruction or unauthorized alteration of data or the IT infrastructure. Examples include: Malware, Phishing, Social Engineering, SPAM, System Attacks, Technology Misuse and Unauthorized Information Disclosure. Report all IT Security Incidents to the Security Operations Center (SOC):
Hotline: +1 877-762-6139    Mailbox: soc@hpe.com
Nestlé Account Security Officer
ASO Role and Responsibilities

– Security governance, compliance, and operations oversight
– Management of security and compliance risks, ensuring that contractual security commitments are met
– Audit facilitation, tracking, remediation, and follow-up
– Security subject matter expert in the course of incident management activities
– Ensure that appropriate security controls & procedures are in place for all services offered to Nestlé
– Measure compliance against security policies and facilitate remediation of areas of non-compliance
– Provide status reports to account and client management on security and compliance

Angel Tatarski
Account Security Officer
HPE Enterprise Security Services

M: +359 888 600 737
T: +359 28 150 359
E: angel.tatarski@hpe.com

Business Park Sofia, B8
Sofia 1766
Bulgaria
Information Security Daily Practice
Security Steps

Please remember:

- Protect sensitive company and client data - the heart of our name and our business.
- Understand and fulfill your security obligations - ignorance is unacceptable.
- Use only approved solutions.
- Secure ALL mobile devices and printed materials - e.g., laptops, phones, REMOVABLE MEDIA.
- Report security incidents IMMEDIATELY.
- Protect your passwords - NEVER share them or write them down.
- Be vigilant toward the dangers of social engineering.
- Use your common sense - if it feels wrong, check it out.
- Dispose of Sensitive Information properly.
- Protect your work location from unauthorised access.
Social Engineering

What is it?

"Social Engineering" is the use of various social skills (such as lying or conning) to attempt to lull a victim into a false sense of security so that they voluntarily reveal information or perform some action that will be useful to an attacker. Social engineering can be carried out over the phone, face to face, or through email. A skilled social engineer will convince you that:

– they are someone they are not and
– there is no harm in giving them the information they are requesting

How to prevent:

Authenticate, Authorize, Call Back, Don't Be Pressured, Be Alert, Be Polite but Firm, Report.

How to respond:

If you believe you are a victim of a social engineering attempt, send an email to global.security@hpe.com and provide them with the details.
Phishing

What is it?

"Phishing" is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to trick the user into surrendering private information. The email directs the user to visit a Web site where they are asked to update personal information (i.e., passwords, credit card information, social security number, bank account number, etc) that the legitimate organization already has. They might even appear to be proper HPE or vendor sites. The Web site, however, is not legitimate and set up only to steal the user's information.

How to prevent:

– Be wary of deceptive emails that appear to be from legitimate sources, especially those who ask you for your password or other sensitive information.

– Always check the address for any suspicious changes or “misspellings” which might not be obvious at a quick glance.

– Do not open suspicious emails, nor click on suspicious links, or attachments.

How to respond:

If you believe you received a phishing email, review this article.
The Headline Test
Designed to consider the soundness and impact of our business decisions

Unsure about a decision or action? Consider the following:
"Before I make a decision, I consider how it would look in a news story."

We should each ask ourselves what the impact would be if the conduct or actions became public or were reviewed by colleagues we respect. If you are uncomfortable with the answer, don’t do it!

– Contact the Ethics and Compliance Office
– Check it with:
  ✓ Your manager
  ✓ Account management
  ✓ corporate.compliance.hpe@hpe.com
  ✓ Legal
  ✓ Human resources
Security Best Practices
“Cheat Sheet” for End-Users

✓ Physically secure your PCs, laptop, USB memory devices, credentials, etc.
✓ Encrypt your PC/Laptop now!
✓ Use strong passwords, never share or disclose.
✓ Have approved anti-malware software running with current definitions.
✓ Do not download suspicious or unapproved software from unsolicited e-mail or high-risk and unfamiliar websites.
✓ Accept PC-COE updates and apply provided security patches as soon as possible.
✓ Protect sensitive information in all forms (electronic, hardcopy, intellectual).
✓ Use collaboration tools securely (e.g. encrypt emails when required, apply access controls on shared files).
✓ Understand and follow HPE security policies and procedures.
✓ Be aware of surroundings and stay alert.
✓ Report incidents to Security Operations Center (SOC).
Useful Links

Nestlé Account Security & Compliance SharePoint site
Nestlé GLOBE Security Policies, Standards and Guidelines
HPE SAP HANA Access Management Guide
HPE-Nestlé Contractual Documentation Collateral
HPE-Nestlé Information Handling Security Guidelines
HPE Standard Software List
HPE IT Policies, Standards and Specifications
Enterprise Security Information System (ESIS)
KeePass Password Management Tool
Latest Version of This Presentation
Thank you

...and remember – HPE is protected by YOU!