THE HOME DEPOT PRIVACY AND DATA SECURITY BEST PRACTICES

Protecting the personal information of The Home Depot's customers and associates and keeping Company information confidential is everyone's responsibility. All associates are expected to adhere to these best practices as well as all other Company policies/SOPs while conducting business on behalf of The Home Depot.

Use secure passwords and protect your passwords

- Your passwords should be complex and should adhere to company standards
- Do not use common "dictionary" words. Instead, use the first letter from each word in an easy-to-remember phrase. For example, based on the phrase "I drive a 1999 Corvette" your password would be ida1999c
- Never share your password and do not allow others to access systems with your credentials (i.e., user ID and password
- Avoid writing down passwords. Never share your password and do not allow others to access systems with your credentials (i.e., user ID and password
- Change your password immediately if you become aware or suspect that your password has been compromised
- Avoid using the same password for work purposes that you do for personal accounts

Protect company-issued hardware and equipment

- If you leave your work area after logging into your computer, ensure the computer is secure and activate the screen lock (Ctrl+Alt+Delete). If your computer does not have a screen lock, log out when you step away. Remember: you are responsible for anything that happens on the computer when you are logged in
- Do not leave your laptop or other company-issued devices unattended in public areas (e.g., airports, crowds, vehicles)
- Limit personal use of Company equipment and avoid storing personal information on Company equipment
- Do not use personally-owned computing equipment to store or process The Home Depot's data or connect to the Company's network (select associates may be approved to perform Company responsibilities using a personal device; you should verify with your manager if you think this applies to you)
- Use only Company approved software on your computer
- Do not load programs, screen savers or games from the Internet or from any non-Home Depot resources
- Immediately report a suspected virus, suspicious program or pop-up, or if your computer exhibits other abnormal behavior to IT Security at IT_Security@homedepot.com (US, Canada and China) or InfoSec@homedepot.com.mx (Mexico)
- Refer to the Use of Cell Phones and Other Electronic Devices (HR SOP EP.028) and ensure compliance with the policy if you are using a mobile device to conduct Company business
- Report loss or theft of IT assets immediately to IT Security at IT_Security@homedepot.com (US,

Canada and China) or InfoSec@homedepot.com.mx (Mexico)

Keep your work space secure

- Wear your ID badge at all times while in the office and do not allow other people to use your badge (non- field associates only)
- Report the loss of your ID badge immediately to the Badging Station at Badging_Station@homedepot.com(SSC Only)
- Escort visitors that have been permitted entry to the office directly where they are required to be
- Do not allow people to "tailgate" behind you when entering secured areas with your badge (i.e., always check to make sure people walking in secured areas are authorized to access those locations with a Company-issued security badge)
- Report suspicious activity and individuals in the office (SSC Only) to the Global Security Operations Center at 770-384-2551 or toll free at 1-877-436-3376

Protect sensitive information

- Do not collect information you do not need; limit the collection of information to only that which is necessary to perform your job responsibilities
- Do not use information for any purpose other than for that which it was originally collected (i.e., use should be limited to what is required to complete the transaction)
- Before sending an email message, fax or text message, confirm the email addresses and fax or phone numbers are correct. Do not include sensitive personal information in email messages, faxed documents, social media websites, text messages or other forms of electronic communication
- When sending files containing personal information via internal e-mail, password protect the file and send the password in a separate e-mail
- Do not store personal information on local hard drives, network shared drives, SharePoint sites, USB flash drives, file-sharing sites (e.g., Dropbox, Box, Google Drive) or other non-Home Depot approved storage areas / tools (select associates may be approved to store personal information on network shared drives; you should verify with your manager if you think this applies to you)
- Keep confidential company documents secured at all times (e.g., in locked filing cabinets or locked rooms)
- Do not discuss confidential Company information (e.g., new products / services not yet publicly announced, internal company communications, financial or earnings related information) in public places
- Do not share personal or Company confidential information with others including coworkers, vendors or other third-parties unless you have obtained approval from your Manager
- If you are a Manager, you may be asked to approve system access requests for your associates. Before you approve a request that grants access to personal information, determine whether the individual requires the access to do their job. Additionally, request that their access is removed when the associate no longer requires it
- Dispose of documents containing personal information or confidential Company information in the designated receptacles in accordance with the Records SOP

Do not become a victim of social engineering or phishing

- Be cautious of requests for personal information which can be received via phone, email or in-person; always confirm the identity and authority of the requestor before providing personal information, especially in response to an unexpected request

- Be aware of phishing scams which are designed to trick individuals into providing personal information in response to phony emails or other requests. Always "think before you click" on links, attachments or images in an email, instant message or on websites. Legitimate emails never ask for personal information such as account credentials (i.e., user ID and password), financial account information or credit card information. Phishing emails often contain poor grammar and spelling errors
- Delete suspicious unsolicited messages without opening
- If you receive a suspicious email to your Company email account, create a new email to @IT_Security@homedepot.com (US, Canada and China) or InfoSec@homedepot.com.mx (Mexico) and attach the suspicious email

Know how to report security or privacy concerns

- To report a data security issue (e.g., lost or stolen laptop, suspicious computer activity) or if you receive a suspicious email to your Company e-mail account, contact IT Security:
    - IT_Security@homedepot.com (US, Canada and China)
    - InfoSec@homedepot.com.mx (Mexico).
- For privacy questions or concerns (e.g., appropriate collection, use, sharing, retention or destruction of personal information), contact the Legal Department:
    - privacy@homedepot.com, 770-433-8211, ext. 18440 (US and China)
    - privacyCanada@homedepot.com, 416-386-5841 (Canada)
    - datopersonales@homedepot.com.mx, +52 (81) 8155-7112 (Mexico)
- Privacy and data security issues can also be reported to the AwareLine:
    - 1-800-286-4909 (US and Canada)
    - 400-800-1046, http://homedepotreport.com (China)
    - 01-800-436-0228 (Mexico)
- Questions regarding data security and privacy can always be directed to your Manager or HR representative

Understand types of data and information

- Personal Information: Information which could be used to uniquely identify an individual (e.g., customer name and address)
- Sensitive Personal Information: Some Personal Information is so sensitive that The Home Depot has additional legal and regulatory obligations to protect it. (e.g., credit card numbers, government issued ID numbers, financial account numbers)
- Confidential Information: Business, financial, sales, marketing and technical information about the Company or its external business partners that could reduce competitive advantage or cause significant financial damage if inappropriately disclosed

Relevant Policies (available on myApron)

- Use of Cell Phones and Other Electronic Devices (HR SOP EP.028)
- The Home Depot Records Management Policy
- The Home Depot Privacy and Data Security Policy (in progress)
- The Home Depot Privacy Policy
- The Home Depot Information Protection Policy
- Information Systems Use and Security (HR SOP EP.015)
- Records Management for Stores (ADM 08-05)

Associate Name:
CHARLES FORD

Date:
01/31/2019

Store/ Location:
0884

Associate ID:
137360525

I understand and acknowledge the Privacy and Data Security Best Practices.

Associate Signature: