Acceptable Use Policy

Department: Information Technology

Effective Date: October 22, 2020

Contents

Purpose

This AUP (Acceptable Use Policy) has been adopted by Dorman Business Consulting (Shanghai) Co., Ltd. to protect Dorman Information from illegal or damaging actions by individuals or entities - either knowingly or unknowingly. This document is intended to support our culture of professionalism, respect, and integrity, in accordance with all applicable law.

Inappropriate use of Company Technology Resources exposes Dorman to risks including, but not limited to: data loss, cyber-attacks, unauthorized access to data (e.g., customer, supplier and Contributor data), interruption of services, and violations of applicable laws, rules and regulations.

Company Technology Resources are to be used for authorized business purposes in serving the interests of Dorman and its stakeholders, including, our customers, suppliers and Contributors. This AUP supplements, and does not replace, Dorman's code of conduct and other applicable policies that may include additional restrictions or obligations with respect to protecting and maintaining Dorman Information.

Scope

This AUP applies to all Dorman Contributors and contractors.

Definitions

AUP – Acceptable Use Policy

ACP – Access Control Policy

BYOD – *"Bring Your Own Device" refers to a*ny technology device not owned by Dorman that is used to send, receive, transmit, or access data/systems owned by Dorman.

Company Technology Resources – Internet/Intranet/Extranet/Cloud related systems, including, but not limited to, computer equipment, mobile phones, tablets, software, operating systems, storage media, network accounts providing electronic communication, email, web browsing, file transfers, and databases, in any event that are owned, leased, licensed or otherwise controlled by Dorman, including to the extent stored in or used on BYOD.

Dorman – Dorman Products, Inc. and its subsidiaries.

Dorman Information – Information, which may or may not be trade secrets, confidential or proprietary information, that is owned or controlled by Dorman, including, but not limited to, customer data, supplier data and Contributor data, whether in the form of messages (e.g., email, text or instant messages), files, documents, software, communications, postings, logins, recordings, or otherwise.

Statement

General Acceptable Use & Ownership

Dorman Information remains the sole property of Dorman, regardless of whether that information is stored on or in Company Technology Resources or other systems or devices owned or controlled by Dorman Contributors, contractors or other third parties.

You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of or access to Dorman Information.

You may access, use, or share Dorman Information only to the extent which is necessary to fulfill your assigned job duties.

Incidental and occasional personal use of Company Technology Resources is permitted as long as it is done on your own time, does not interfere with the work of others, does not interfere with network bandwidth, and is not considered a prohibited activity under Dorman policies or applicable law. You are responsible for exercising good judgment when using Company Technology Resources.

Dorman permits, but does not require, the use of BYOD computers, smart phones and tablets to perform work for or on Dorman's behalf. However, any use of a personal device for business purposes must conform to this AUP. In addition, you are responsible for using your devices in a sensible, productive, ethical, and lawful manner and remain responsible for all expenses related to personal devices, unless otherwise required by applicable law. This AUP applies to work performed on any BYOD for or on behalf of Dorman during working and nonworking hours, on and off Dorman premises.

Expectations of Privacy

Company Technology Resources

(i) Dorman reserves the right to at any time monitor, intercept, review, and erase, without further notice, all Dorman Information or the entire contents of any Company Technology Resource in its sole discretion.

(ii) This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing of transactions, messages (e.g., email, text or instant messages), communications, postings, logins, recordings, and other uses of the device.

(iii) Therefore, you should have no expectation of privacy regarding Dorman Information stored on or in Company Technology Resources, subject to applicable law.

(iv) Dorman will provide advance notice where possible and will take reasonable

precautions to avoid the loss of your personal content that may be stored on or in any Company Technology Resource when any such the device is erased. It is your responsibility to regularly back up your personal content so that you do not lose personal information if any such device is erased.

(v) Dorman may also make and preserve copies of all Dorman Information and, with respect to any Company Technology Resource, copies of the entire contents of such device or system. Furthermore, Dorman may delete those copies from time to time without notice.

(vi) In addition, any and all contents of Company Technology Resources, including information that is not Dorman Information, may be obtained and used for litigation, investigations, to the extent consistent with applicable law.

BYOD

While Dorman does not monitor or have access to personal data, communications, or applications on any BYOD - the following requirements apply:

(i) To protect Dorman Information stored on or in your BYOD, you are required to notify Dorman immediately if any of your BYOD resources containing Dorman Information is lost, stolen, accessed by unauthorized persons, or otherwise compromised so Dorman can assess the risk and, at Dorman's sole discretion, erase all or part of the Dorman Information contained on or in the device.

(ii) You must also promptly provide Dorman with reasonable access to your BYOD when requested or required for legitimate business purposes, including in the event of any security incident or investigation.

(iii) To the extent Dorman determines that the Dorman Information stored on or in your BYOD must be erased, Dorman will provide advance notice where possible and will take reasonable precautions to avoid the loss of your personal content that may be stored on your BYOD. It is your responsibility to regularly back up your personal content so that you do not lose personal information if any such device is erased.

(iv) Dorman may also make and preserve copies of all Dorman Information included on

your BYOD and may delete those copies from time to time without notice. Any such Dorman Information may be obtained and used for litigation and investigations, to the extent consistent with applicable law.

(v) Your use of any BYOD for or on behalf of Dorman is at your own risk and Dorman will not be responsible for any losses, damages, or liabilities arising out of the use of any BYOD under this AUP - including any loss, corruption, or use of any content or loss of access to or use of any device, its software, or its functionality.

General Security Requirements and Data Handling

With respect to any Company Technology Resource or any BYOD containing Dorman Information, you are expected to do the following:

Lock the screen or log off a computer or mobile device before leaving it unattended.

Keep usernames and passwords confidential – providing access to another individual, whether a family member, administrative assistant or otherwise, either deliberately or through failure to secure its access, is prohibited.

Do not open email messages from unknown senders or with attachments or weblinks that you are not expecting, even if you know the sender, as these can be malware. Instead, contact the sender or the Dorman information technology services group to determine if the email is legitimate.

Use your best efforts to physically secure the device against loss, theft, damage, or use by persons who have not been authorized to access the device by Dorman.

Do not transmit Dorman Information over an unsecured public WiFi network.

With respect to BYOD on which Dorman Information is stored, you must:

(i) register the BYOD with Dorman's information technology services department so that it can be authorized for use.

(ii) install Dorman's approved Mobile Device Management Software on the BYOD to enforce data encryption and updated operating system versioning, and any updates that may be requested by Dorman from time to time.

(iii) not backup Dorman Information locally or to cloud-based storage services without Dorman's consent.

Unacceptable Use

Under no circumstances are you permitted to use Company Technology Resources or any BYOD containing Dorman Information for any illegal activity under applicable laws or regulations.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

(i) Infringement of Dorman's or another party's intellectual property rights, such as

copyrights, trademarks, trade secrets, confidential and proprietary information, and patents.

(ii) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Dorman or you do not have an active license.

(iii) Accessing data, a server or an account for any purpose other than conducting Dorman business, even if you have authorized access, is prohibited.

(iv) Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

(v) Procuring or transmitting material that is in violation of Dorman policies and applicable law, including prohibitions on discrimination, harassment, including sexual harassment or a hostile workplace, and retaliation.

(vi) Making fraudulent offers of products, items, or services.

(vii) Initiating of or aiding in security breaches or disruptions of network communication.

(a) Security breaches include, but are not limited to, accessing data of which you are not an intended recipient or logging into a server or account that you are not expressly authorized to access, unless these duties are within the scope of your regular duties.

(b) For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

(viii) Port scanning or security scanning prohibited unless prior notification to the information technology department is made.

(ix) Executing any form of network monitoring that will intercept data not intended for your host, unless this activity is a part of your normal job responsibilities.

(x) Circumventing user authentication or security of any host, network or account.

(xi) Introducing honeypots, honeynets, or similar technology on the network.

(xii) Interfering with or denying service to any user other than your host (for example, denial of service attack).

(xiii) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

(xiv) Providing information about, or lists of, Dorman Contributors to parties outside the organization who do not have a contractual or other right to receive it in accordance with Dorman's policies.

Email Communication Activities

When accessing and using the Internet for communications in connection with your job responsibilities, you will be seen by others as a representative of Dorman. Accordingly, you are prohibited from:

(i) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

(ii) Engaging in any form of harassment or other unprofessional conduct via email, instant message, telephone, facing or otherwise, whether through language, frequency, or size of messages.

(iii) Using without authorization, or forging, of email header information.

(iv) Inappropriately soliciting email for any other email address, other than that of the poster's account.

Compliance

Audit / Compliance Measurement

Compliance with this AUP may be verified through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Non-Compliance

Violation of this AUP will be regarded as a serious breach of the policies of Dorman Business Consulting (Shanghai) Co., Ltd. and subject to disciplinary action, including, but not limited to, termination of employment.

Controls

All changes to Policy Level IT documentation must be authorized by the Director, Enterprise Technology or the Senior

Vice President, Chief Information Officer.

Revision History

Change Owner	Summary of Change	Change Approver	Approval Date	Change Date
Zack Varaly	New Document	Donna Long	10/22/2020	10/22/2020
Zack Varaly	Content Review	Donna Long	11/30/2022	10/20/2022

Related Documents

Document Title	Document Description	Link to Document
N/A	N/A	N/A