THE HOLST GROUP DATA PROTECTION POLICY FOR COLLEAGUES – May 2018

This policy applies to all personal data held by The Holst Group in both manual and electronic formats.

It is the Colleague's responsibility to read, comply with and keep updated with all relevant The Holst Group Data Protection Policies including:-

- Data Protection Policy (separate document)
- Privacy Notice (separate document)
- Data Destruction Policy (separate document)
- Subject Access Request Policy (separate document)
- Cookie Policy (separate document)
- Password Policy (Below)
- Clean Desk Policy (Below)

PASSWORD POLICY

Overview
This policy is intended to establish guidelines for effectively creating, maintaining, and protecting passwords at The Holst Group.

Scope
This policy shall apply to all employees, contractors, and affiliates of The Holst Group, and shall govern acceptable password use on all systems that connect to The Holst Group network or access or store The Holst Group data.

Policy
Password Creation

1. All user and admin passwords must be at least [8] characters in length. Longer passwords and passphrases are strongly encouraged.
2. Where possible, password dictionaries should be utilized to prevent the use of common and easily cracked passwords.
3. Passwords must be completely unique, and not used for any other system, application, or personal account.
4. Default installation passwords must be changed immediately after installation is complete.

Password Aging

1. User passwords must be changed every 3 months. Previously used passwords may not be reused.
2. System-level passwords must be changed on a quarterly basis.
3. Please see Last Pass section regarding shared sites.

Password Protection

1. Passwords must not be shared with anyone (including co-workers and supervisors), and must not be revealed or sent electronically.
2. Passwords shall not be written down or physically stored anywhere in the office.
3. When configuring password "hints," do not hint at the format of your password (e.g., "postcode + middle name")

4. User IDs and passwords must not be stored in an unencrypted format.
5. User IDs and passwords must not be scripted to enable automatic login.
6. “Remember Password” feature on websites and applications should not be used.
7. All mobile devices that connect to the company network must be secured with a password and/or biometric authentication and must be configured to lock after 3 minutes of inactivity.

Enforcement
It is the responsibility of the end user to ensure enforcement with the policies above.
If you believe your password may have been compromised, please immediately report the incident to Iain Chalmers and change the password.

Last Pass

The Holst Group has provided colleagues with access to Last Pass – this enables all shared access sites to be accessed by the individual.

The Admin team will be responsible for updating the shared site passwords. If the individual chooses to use Last Pass for your individual access to sites used for The Holst Group purposes, it is their responsibility to update passwords regularly and in line with this policy.

Colleague’s must log out of Last Pass when they leave their desk and shutdown their computer at the end of each working day.

Clean Desk Policy

Overview

The Holst Group stands committed to the development of secure policies and practices, and in doing so, has implemented this Clean Desk Policy to increase physical security at The Holst Group locations. This policy ensures that confidential information and sensitive materials are stored away and out of sight when they are not in use or when the workspace is vacant.

This policy sets forth the basic requirements for keeping a clean workspace, where sensitive and confidential information about The Holst Group employees, clients, vendors, and intellectual property is secured.

The policy shall apply to all The Holst Group employees, contractors, and affiliates.

Policy

Employees are required to secure all sensitive/confidential information in their workspace at the conclusion of the work day and when they are expected to be away from their workspace for an extended period of time. This includes both electronic and physical hardcopy information.

Computer workstations/laptops must be locked (logged out or shut down) when unattended and at the end of the work day. Portable devices like laptops and tablets that remain in the office overnight must be shut down and stored away.

Mass storage devices such as CD, DVD, USB drives, or external hard drives must be treated as sensitive material and locked away when not in use.

Printed materials must be immediately removed from printers or fax machines. Printing physical copies should be reserved for moments of absolute necessity. Documents should be viewed, shared and managed electronically whenever possible.

All sensitive documents and restricted information must be placed in the designated shredder bins for destruction. Please refer to the Data Destruction Policy for additional information pertaining to document destruction.

File cabinets and drawers containing sensitive information must be kept closed and locked when unattended and not in use.

Passwords must not be written down or stored anywhere in the office.

Keys and physical access cards must not be left unattended anywhere in the office.

It is the responsibility of each colleague to ensure enforcement with the policies above. Repeated or serious violations of the clean desk policy can result in disciplinary actions.

If you notice that any of your devices or documents have gone missing, or if you believe your workspace has been tampered with in any way, please notify Iain Chalmers immediately.

Colleague Actions:

Password Protection Actions:

Please follow the links/instructions below to assist with points 5 & 6 under Password Protection.

To stop Chrome asking for passwords - https://www.laptopmag.com/articles/disable-chrome-passwords

To stop Firefox asking for passwords – https://www.itsupportguides.com/knowledge-base/tech-tips-tricks/firefox-how-to-stop-save-password-prompt-disable-password-manager/

Delete cookies (and therefore saved passwords) – https://support.google.com/accounts/answer/32050?co=GENIE.Platform%3DDesktop&hl=en

Set Chrome to auto log out GMAIL on exit - Ctrl Shift Delete (MAC:Command/Shift/Backspace) - delete all passwords from beginning of time. Then Settings/Advanced/Manage Passwords - set to OFF

Sign Off:

Please print your name, sign and date this document to confirm that:

1) You have read this Policy and understand your responsibilities with regards to Data Protection
2) You have Completed the **Password Protection Actions** above

Colleague Name: ……

Signed: ……

Date: ……