Google Glass Policy Template

Janco Associates, Inc.

2023 Edition

Table of Contents

Google Glass Policy

Overview

The purpose of this policy is to define standards, procedures, and restrictions for Google Glass and other wearable cameras and recording devices.

There are clear benefits and risks to these devices in the workplace.

- They can be used for alerts and notifications as pagers and smartphones. Wearers can g to do whatever it is they
- during work will benefit hite-collar worker sitting
- ct the wearer to perform
- It will prove to be a benefit to the visually impaired and other disabled employees.

The policy applies to any device that could be used in such a manner, even when the equipment is not approved, owned, or supplied by ENTERPRISE.

Policy

Use of Google Glass and other wearable camera and recording devices is allowable under the following conditions:

- The privacy and confidentiality of Enterprise facilities, systems, information, property, employees, guests, suppliers, and customers are maintained.
- Devices will not be used in any manner that compromises any individual or processes at enterprise locations.
- If the device is enterprise-owned and approved, it is not to be used away from enterprise locations unless it is specifically authorized by the enterprise.

There can be limited personal use of the device:

- Imposes no tangible cost on ENTERPRISE;
- Exposes ENTERPRISE to any liability or risk;
- Does not unduly burden the ENTERPRISE's computer or network resources;
- If it has no adverse effect on an employee's job performance

Upon entry in any location noted with a sign that Google Glass devices are not permitted, the device should be removed and powered off.

All users shall be required to acknowledge receipt and understanding of all regulations governing the use of Google Glass and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with ENTERPRISE policies.

Google Glass Security Best Practices

For Google Glass, content management includes robust security, and device management capabilities are the definition of best practices. CIOs and CSOs should implement the following:

General

- Be wary of QR codes, especially if you're being pressured to use them such as for a contest.
- Don't connect to open networks/only connect to trusted secured networks

to tether with for online access

d returned be prepared to erase
ugh your Google account.

from Google.

ements and get familiar with

Security Controls

- 256-bit AES encryption per file at rest, 30-day rotating encryption key - Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. It has been adopted by the U.S. government and is now used worldwide.
- 256-bit SSL encrypted data transfer - 256-bit SSL Encryption provides an extra layer of protection for our users. This protection can help defend against login and password theft, which is particularly common in today's wireless society.

Remote Google Glass Management

- At least a 4-digit passcode for each device
- Immediate access restriction on the device
- Automatic login to end-user accounts which includes the facility to remotely wipe all data and software from the device
- Automatic shutdown and locking of a device after a security breach from a device
- Security breach reporting

Appendix – Electronic Forms

Three (3) Electronic forms are included with this policy template. They come separately in their own directory.

- Google Glass Access and Use Agreement
- Mobile Device Access and Use Agreement
- Mobile Device Security and Compliance Checklist
- Wearable Device Access and Use Agreement

What's New

2023 Edition

- Updated all attached electronic forms
- Updated to comply with the latest mandated requirements

2022 Edition

- Updated all attached electronic forms
- Updated to comply with the latest mandated requirements

2021 Edition

- Added form -Wearable Device Access and Use Agreement
- Updated all attached electronic forms
- Added section on ownership of device and data
- Updated WFH materials

2020 Edition

- Added Work From Home and tele-meeting considerations
- Added Mobile Device Access and Use Agreement
- Mobile Device Security and Compliance Checklist
- Proved a separate copy of the latest Google Glass Use and Agreement From