



UNITED STATES MARINE CORPS
MARINE CORPS UNIVERSITY
EDUCATION COMMAND
2076 SOUTH STREET
QUANTICO, VA 22134-5129

IN REPLY REFER TO
2201

CG
NOV 06 2020

MARINE CORPS UNIVERSITY/EDUCATION COMMAND POLICY LETTER 4-20

From: Commanding General, Education Command
To: Distribution List

Subj: MARINE CORPS UNIVERSITY USER POLICY REGARDING GOOGLE SUITE

Ref: (a) Marine Corps Bulletin 5200 (Marine Corps Digital Signature & Encryption Policy)
(b) Marine Corps Bulletin 5210 (Policy for Email Usage, Email Account Management, and Records Management on MCEN NIPRNET)
(c) Google for Work Security and Compliance Whitepaper
(d) MCU Naming Standards for Applications, Network and Systems SOP (18 Dec 13)
(e) Do-It-Yourself (DIY) Instructions for Setting Up Google Apps Sync for Microsoft Office (Oct 15)

Encl: (1) Marine Corps University User Policy Regarding G Suite Frequently Asked Questions (FAQs)
(2) MCU Education (.EDU) Network User Agreement (MDM Excerpt)

1. Purpose. To implement policy for the usage of Google Suite (G Suite) across Marine Corps University (MCU) and applicable stakeholders.
2. Background. In conjunction with the implementation of the MCU Education (.EDU) Network at the Warner Center, as well as multiple current resident sites across Marine Corps Base (MCB) Quantico and remote locations to include MCB Camp Johnson, MCU has adopted a commercially hosted cloud-service provider (G Suite). This technology provides a collaboration suite more conducive to MCU's education-focused environment and decreases long-term Information Technology (IT) costs. This effort marks a significant change to familiar e-mail, calendar, shared drive, and intranet systems. User questions and concerns should be initially addressed in Enclosure (1) Marine Corps University User Policy Regarding Google Suite (G Suite) FAQs.
3. Policy. MCU has been granted an Authority to Operate (ATO) from Headquarters Marine Corps Command, Control, Communications and Computers (HQMC/C4) that mandates compliance with Department of Defense (DoD) Information Assurance policies. Specific policy items are addressed in the following sections pertaining to the following functional topics: (1) Administration and Security; (2) G Suite Applications; (3) Integration with Microsoft Outlook; (4) Mobile Device Management (MDM); and (5) Support for Bring Your Own Device (BYOD).

a. Administration and Security

(1) Ownership and Use of Data. The DoD owns the email, calendar, files, and other data within the Google USMCU.EDU domain, and all services provided are managed by MCU IT. Google is required to comply with all applicable privacy laws; and the DoD agreement with Google specifically requires Google to comply with the Federal Information Security Management Act (FISMA) when handling data that includes MCU student information and to maintain their FEDRAMP accreditation.

(2) Prohibition of Data Mining. Per the licensing agreement, Google's use of MCU data is limited to only that which is necessary for Google to provide the services required by MCU. Google may not scan or mine MCU data for advertising or other purposes. Google is contractually prohibited from serving advertisements in the MCU G Suite environment.

(3) Scanning and Indexing. In order to provide essential core features for MCU Email, Google will run fully automated scanning and indexing processes to offer improved spam filtering, virus detection, and email search, just as MCU IT currently does for the .EDU network for the same purposes.

(4) Additional Information. For more information about Google's security, visit "Google Privacy of Terms": <https://policies.google.com>.

(5) Administrative Privileges. Select personnel within MCU IT will have elevated administrative privileges to manage unique system settings as outlined below. MCU personnel will be able to resolve all system administration issues by visiting or contacting the IT Helpdesk (703-432-4866 or helpdesk@usmcu.edu).

(6) Account Management. One significant difference from Marine Corps Enterprise Network (MCEN) is that .EDU account management is a responsibility of MCU IT.

(a) Account Creation. MCU IT/Customer Support Branch (IT Helpdesk) will create all accounts for G Suite. In accordance with MARADMIN 698/13, completion of Cyber Awareness training remains a requirement to gain access onto MCU's .EDU Network. As the inherent email, calendar, shared drive collaboration system for the .EDU Network, a single System Authorization Access Request will suffice for .EDU and G Suite.

(b) Account Access. Using their government issued Common Access Card (CAC) or Alternate Tokens (ALT tokens), users will be able to access their email, calendar, contacts, shared drive, and other G Suite tools through approved web browsers (See Enclosure (1) for details).

(c) Account Termination. All MCU personnel shall check-out with MCU Information Technology (IT) before departing the command. Upon leaving MCU, personnel will have 30 days to back-up their own files via file download or by burning a DVD back-up disc. MCU will retain personnel records in accordance with (IAW) Reference (b).

(d) MCEN & .EDU Account Co-existence. The .EDU network is the primary network for MCU. It is not desired to actively maintain accounts in both MCEN and .EDU, but

this is an inevitable end-state for limited, case-by-case sections (e.g., personnel requiring regular access to Marine Corps Total Force System (MCTFS/3270), Standard Accounting, Budgeting and Reporting System (SABRS), Global Combat Support System Marine Corps (GCSS-MC), Defense Civilian Pay System (DCPS)). New personnel transitioning to .EDU as their primary network (e.g., faculty, students, and academic services) should minimize their time in transition in accordance with commercial best practices.

(7) Cyber Security

(a) Privacy and Security of G Suite. Google has provided assurance that its policies regarding data center access and server access are appropriate and consistent with how DoD controls access to servers and data centers.

(b) Data Center Standards. Google is contractually and legally obligated to protect MCU's data and to adhere to DoD standard systems and procedures regarding security and confidentiality. Google will store MCU data in server facilities located within the United States.

(c) For Official Use Only (FOUO) and/or Sensitive but Unclassified (SBU) Material. Standing DoD and USMC policy applies for the .EDU network and storage and transmission G Suite of FOUO and/or SBU material. This includes Personally Identifiable Information (PII) or Personal Health Information (PHI). As a general practice, users should avoid transmitting sensitive data in email. **Users shall not download FOUO, SBU, PII, or PHI information to any personally owned devices.**

(d) Encryption of Data at Rest (DAR). Data stored on the cloud (for the purposes of this policy at Google Data Centers) will adhere to DoD data encryption standards. DAR will be encrypted using the approved third party applications and actively monitored by MCU IT Cybersecurity personnel.

(e) Digital Signature & Encryption of Email. MCU personnel will continue to digitally sign and/or encrypt email traffic in accordance with USMC policy (Reference (a)).

b. G Suite Applications. Several cloud-based applications come organic or as third-party add-ons with MCU G Suite licenses. Please note that not every application in G Suite is approved for use.

(1) Available Applications

(a) Google Mail. Users will be equipped with all of the common email features they are accustomed to in modern email systems. They will also be able to customize their settings as desired using the many tools provided within the browser and user interface (e.g., themes, labs, labels, etc.).

(b) Google Calendar. Calendars are by default shareable across the USMCU.EDU domain. Users will be able to share calendars external to the USMCU.EDU domain within G Suite, but only on a read-only basis.

(c) Google Drive. This element of G Suite servers as a highly collaborative file management and collaboration feature. Every user has an unlimited amount of cloud storage for use. **Please note that sharing from the Drive outside of the .EDU organization is prohibited and blocked by the system.** MCU users will have access to the applications listed below that are organic to Google Drive. These applications are advantageous in allowing real-time collaboration for as many as 50 users who have been granted access to the file; and they mirror typical word processor, numbers processor, and presentation software. Of note, MCU users will always be provided the familiar suite of equivalent Microsoft Office applications (e.g., Word, Excel, and PowerPoint) on their government-provided clients.

- Google Shared Drives
- Google Docs
- Google Sheets
- Google Slides
- Google Forms
- Google Drawings

(d) Google Groups. Select users can create a Group within the USMCU.EDU domain in G Suite. Most Groups will be private to the domain; exceptions will include public facing email addresses (e.g., MCU_Press@usmcu.edu, MCU_Web_Inquiries@usmcu.edu, etc.). There are four types of Groups that can be created in G Suite; more information can be found in the FAQs enclosure.

- Email List
- Web-based Forum
- Question & Answer Forum
- Collaborative Inbox

(e) Google Contacts. Aside from the ability to type in a contact's email address, users will have immediate access to all USMCU.EDU domain members as well as existing contacts should they choose to import them from their Outlook archive or any applicable comma-separated variable (CSV) or vCard file.

(f) Google Sites

(g) Google Chat. Accessible within the .EDU network only.

(h) Google Meet. Google Business version of Hangouts. Allows Video Meetings with people inside or outside of the organization. Also provides a dial-in number with PIN. Meeting may also be scheduled from Google Calendar.

(i) Google Keep

(j) Google Forms

(2) Unavailable Applications

(a) Collections

(b) Google+

(c) Google Apps Marketplace

4. Approved Additional/Third Party Applications

a. Cloudlock. Invisible to most users, this application provides MCU administrators the ability to comply with FOUO and PII sharing policies and will auto-generate potential breach alerts to MCU Cybersecurity personnel. IT personnel will monitor these alerts and will notify users if any immediate action is required to minimize potential exposure events.

b. Vault. Invisible to most users, Vault is an add-on to retain, archive, search, and export your organization's email and on-the-record chats for eDiscovery and compliance needs.

5. Collaboration Security

a. Sharing External to .EDU. Sharing Google Drive folders and files within and outside the USMCU.EDU Domain is not authorized. To mitigate the risks of PII spillages or HIPAA incidents, G Suite automatically scans for PII and HIPAA data. If found, the system automatically blocks email and sends the sender a notice. Users are also prohibited from blanket sharing their entire Google Drive with external domains. In some instances, users may receive limited information sharing capacity (to within the USMCU.EDU domain only) if any potential information security risk is greater than the realized benefit. This measure will be implemented primarily for transitory personnel and high-risk users and is in place to assist with spillage containment or FOUO control. Users will always have the ability to email/download non-classified documents to their personal account/device. However, **users shall not download or share FOUO, SBU, PII, or PHI information to any personally owned devices.**

b. Ownership Transfer. Google Groups, Sites, and Calendars that are owned by individual G Suite users can be transferred by the owner of MCU's G Suite Administrators by visiting or contacting the IT Helpdesk.

c. Google Drive for Mac/PC. Google Drive for Mac/PC is not enabled with MCU's G Suite licenses in order to minimize incidental uploads.

d. Offline Data Access. Offline data access is disabled for MCU users to alleviate potential FOUO/PII breach incidents as well as version control and inadvertent over-write issues.

6. Naming Conventions. Naming conventions for email will be IAW Reference (d) with the following additions:

a. Email. MCU G Suite email addresses will be first.last@usmcu.edu for active duty or government personnel. Contractors will have the additional ".ctr" following their last name (first.last.ctr@usmcu.edu). Foreign Service personnel will have additional letter annotating their country in a similar fashion. Middle initials will be included to further delineate personnel with the same first and last name, followed by the addition of a numeral at the end of the email address prefix as required.

b. Calendars, Groups, and Sites. Google Calendars, Groups, and Sites will be named according to school/directorate and section. For example:

- MCU_IT_Helpdesk
- MCU_CSC_CG04
- MCU_HD_Archives

7. User Avatars. MCU G Suite users are authorized to maintain a professional photo as their user avatar.

8. Re-directing of MCEN to .EDU. Users with MCEN accounts can re-direct their MCEN email to their Google email account by calling the Marine Corps IT Support Center (North Capital Region) Helpdesk at (703) 784-2111. Of note, this is not a rule a user can enact within Microsoft Outlook on a user's MCEN account as it must be completed on the Exchange Server. Additionally, emails sent to the user's .MIL address will *only* appear in their Google email once auto-forwarding is established in this fashion.

a. Integration with Microsoft Outlook. Despite inherent proprietary incompatibility across the industry, Google and Microsoft have provided rudimentary means for collaboration. Users who desire to continue to maintain their .EDU email, calendar, and contacts on the Microsoft Outlook user-interface are able to do so via Google Apps Sync for Microsoft Outlook (GASMO). Do-It-Yourself (DIY) Instructions for setting up this feature are available at the IT Helpdesk and have been disseminated across the command (Reference (e)).

b. Mobile Device Management (MDM). MCU is implementing MDM as an *optional* capability for the integration of G Suite applications on users' mobile devices. For purposes of this policy, mobile devices constitute portable electronic devices smaller than laptop computers (e.g., tablets, phablets, and smartphones). Users interested in enabling MDM on a personal mobile device should contact the IT helpdesk for guidance on configuration. Note there is a max of two devices per user.

9. Compatible Systems. MCU IT will update compatible systems for MDM with each update of G Suite FAQs for publishing on the MCU public-facing website. Of note, in electing to implement MDM on a personal device a user will not see any impact on other Google accounts registered to the device. The standard practice for compatible systems is at least the latest two versions of operating systems.

10. MDM Security. Users electing to implement G Suite applications on their mobile device will have their device encrypted. Likewise, should the user lose, sell, or upgrade their physical device (not merely updating the Operating System), they will be subject to having their device deleted, or even wiped in extreme situations by MCU IT. IT Helpdesk personnel will be able to fully outline this process throughout the MDM implementation process.

11. MDM Limitations. While the employment of G Suite MDM provides a significant increase in technological mobility for the typical user, this capability also poses distinct limitations. MDM does not provide users with access to their PKI certificates residing on their CAC. In turn, users will typically have difficulty in accessing digitally signed or encrypted emails.

12. Mandatory MDM Settings. Certain system settings are mandated for users should they elect to deploy G Suite applications on their mobile device. These settings are largely benign (e.g., mandatory download of the Google Apps Device Policy application, mandatory PIN establishment of the user's choice, device auto-lock after five minutes of inactivity, and will automatically wipe device after 10 failed password attempts) and will not interfere with the operation of the device. Helpdesk personnel will be able to fully outline these system constraints during initial set-up.

13. User Agreement (UA)

a. Enclosure (2) is the MCU IT MDM user agreement. All personnel will be required to acknowledge this section of this UA during the account creation process. A copy of the signed document is available upon request.

b. Support for Bring Your Own Device (BYOD). MCU IT will provide initial support for faculty, staff, and students for establishing and maintaining access to their government-issued G Suite accounts. This support will be limited in scope and will comprise primarily of initial set-up of personal devices.

14. Applicability. This Policy is effective immediately and applies to G Suite users across all Schools, Colleges, and Directorates of Marine Corps University.



J. M. BARGERON

Distribution:

Vice Presidents

Director, Marine Corps War College

Director, School of Advanced Warfare

Director, Command and Staff College

Director, Expeditionary Warfare School

Director, College of Enlisted Military Education

Director, National Museum of the Marine Corps

Director, Lejeune Leadership Institute

Director, History Division

Director, Marine Corps University Press

MARINE CORPS UNIVERSITY USER POLICY REGARDING GOOGLE SUITE (G SUITE)

FREQUENTLY ASKED QUESTIONS

1) Why is MCU implementing G Suite?

MCU has pursued a commercially-hosted cloud service provider in order to provide a collaboration suite more conducive to MCU's education-focused environment and decrease long-term Information Technology costs. This effort marks a significant change to familiar DoD provided e-mail, calendar, shared drive, and intranet systems. It also puts MCU on a similar footing with other DoD PME-focused organizations as well as civilian institutions of higher education.

2) What does "Cloud-service" really mean?

Cloud service is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than utilize a local server or a personal computer. Email services through Gmail, Yahoo, AOL, or Hotmail are all commercially provided cloud services.

3) Who will get a G Suite Account?

G Suite accounts will be furnished for all staff, faculty, and students across MCU that have access to the .EDU Network.

4) What "Apps" do I get with G Suite?

Each user will receive access to several organic and third-party applications:

- Gmail (<http://mail.usmcm.edu>)
- Drive (<http://drive.usmcm.edu>) including Shared Drives
- Calendar (<http://calendar.usmcm.edu>)
- Sites (<http://sites.usmcm.edu>)
- Groups (<http://groups.usmcm.edu>)
- Google Docs
- Google Contacts
- Google Sheets
- Google Slides
- Google Forms
- Google Drawings
- Google Meet
- Google Chat (within .EDU only)
- Google Keeps
- Google Forms
- Google Vault (limited to administrators)
- Cloudlock (limited to administrators)

5) What "Apps" do I NOT get with G Suite?

The following Google applications/capabilities are currently not available for MCU G Suite Users:

- Google+
- Google Collections
- Google Apps Marketplace

6) Can I still use MS Office programs?

Yes, Microsoft Office is still available as a suite of desktop applications (Word, Excel, PowerPoint, Access, and Outlook) on all .EDU devices furnished by MCU IT. However, Google Apps provides an easy-to-use suite of desktop applications that enables collaboration between users (Docs, Sheets, Slides, Forms, and Drawings). Compatibility between these programs is simple via the standard "Save As..." functionality within most programs.

7) What files are compatible if I desire to use Google's organic applications/Software as a Service (SaaS) instead of Microsoft Word, Excel, or PPT?

Please note that file types from Microsoft Office 2013 or newer are compatible. Below are the some of the compatible file types that can be converted to a Google document, spreadsheet, or presentation:

- For documents: .docx, .docm, .dotx, .dotm, .html, plain text (.txt), .rtf, .odt, .xml
- For spreadsheets: .xlsx, .xlsm, .xlsb, .xlt, .xltx, .xltm, .ods, .csv, .tsv, .txt, .tab
- For presentations: .pptx, .pptm, .pps, .ppsx, .ppsm, .pot, .potx, .potm, .odp

MARINE CORPS UNIVERSITY USER POLICY REGARDING GOOGLE SUITE (G SUITE)

- For drawings: .wmf
- For Optical Character Recognition (OCR): .jpg, .gif, .png, .pdf

- 8) **Are there any file formats that are explicitly not supported that should be mentioned up front?**
Microsoft Office extension from versions older than 2013.
- 9) **How do I log in?**
Users will be required to log-in to their .EDU system using their Common Access Card (CAC) or Alternate Token (alt-token), giving them access to their profile/desktop. They will then need to open an internet browser (e.g., Internet Explorer, Chrome, and Firefox) and navigate to <https://mail.google.com/a/usmcu.edu> where they will be prompted to select their CAC email certificates in order to access their Google profile.
- 10) **Will I have two email accounts?**
MCU users in some instances will have two accounts, or account “co-existence.” This is not the desired or recommended long-term solution, but rather reflects the required special cases.
- 11) **Can I still use Microsoft Outlook as my “User Interface”?**
While it is possible to manage google accounts via Google Apps Sync for Microsoft Outlook (GASMO) into Microsoft Outlook, it is not recommended. The standard user interface that MCU will implement and support will be a web browser for the following reasons:
- Newest features available.
 - Consistent access from anywhere.
 - Seamless App integration.
 - Speed.
 - Security & availability.
 - Search capabilities.
- 12) **Can I access my Outlook PST Files in G Suite?**
Yes. Old .PST files can still be accessible in Microsoft Outlook but with limited capability and interoperability. You will be able to see your old emails and attachments by opening the Outlook application.
- 13) **Which browser should I use?**
- Short answer: Chrome (preferably); Firefox; IE.
 - Google’s *Chrome* browser is recommended for the best Google Apps experience. This will serve as the primary means to access Google emails, calendar, sites, and drive (including docs, sheets, slides, forms, and drawings).
 - Government-issued devices will be configured in this manner.
 - For BYOD devices, IT Help Desk is available to assist in the installation and configuration of these browsers. G Suite will also work on other browsers (Internet Explorer, Opera, and Safari).
 - Of note, Microsoft discontinued Internet Explorer in 2016.
- 14) **Will my .EDU account (G Suite Gmail account) be seen on the Marine Corps’ Global Address List (GAL)?**
Yes. In fact, there will likely be a period of time in which your MCEN and .EDU accounts both appear in the GAL.
- 15) **How will I be trained on Google Apps?**
Training is available through the Google Apps Learning Center, <http://learn.googleapps.com>. This site is maintained by Google, so you will continue to have the most updated training videos and information as it is released. Research indicates that individual users quickly adapt to the new capabilities inherent to G Suite.
- 16) **Where do I get support with G Suite issues?**
Call the MCU IT Helpdesk at 703-432-4866 or email HelpDesk@usmcu.edu with any G Suite issues. Personnel at the Helpdesk have training in G Suite and will be able to perform triage as required to elevate a trouble ticket.
- 17) **Can I still digitally sign / encrypt my email?**
Yes, and the requirements to follow Marine Corps policy in this regard do not cease for users within the .EDU Network or through G Suite.

MARINE CORPS UNIVERSITY USER POLICY REGARDING GOOGLE SUITE (G SUITE)

USMC Policy on signing/encrypting emails:

1. Only sign if required
2. Digitally Sign if sending attachments/hyperlinks
3. Encrypt if FOUO, SBU information is contained in the email:
 - Any contract sensitive information.
 - Privacy Data, Personally Identifiable Information.
 - Employee's Personnel File.
 - Any medical or health data.
 - Operational data regarding status, readiness, location, or deployment of forces or equipment.

Users can digitally sign and encrypt your emails via Microsoft Outlook. While users will always be able to receive help at the IT Helpdesk, MCU IT will publish a "gouge book" to allow personnel a Do-It-Yourself help option.

Of note, the ability to simply share files across Google Drives within the .EDU network will for most users eliminate the need to frequently send attachments or digitally sign/encrypt emails.

18) Is my data safe?

Yes, your data is safe. G Suite includes dozens of security features specifically designed to keep your data safe and secure within CONUS based data centers. G Suite was the first cloud-based email application to receive Federal Information Security Management Act (FISMA) accreditation from the U.S. federal government. G Suite offers an extra layer of security with two factor authentication, greatly reducing the risk of usernames and passwords being stolen. Google guarantees an SLA of 99.9% availability with zero scheduled down-time.

Google data centers are SSAE 16 / ISAE 3402 Type II, SOC 2-audited and have achieved ISO 27001 certification. For industries or geographies subject to specific regulations, Google Drive supports FISMA, Family Educational Rights and Privacy Act (FERPA), and Health Insurance Portability and Accountability Act (HIPAA) and adheres to the Safe Harbor Privacy Principles.

19) Can I access my Google account on a Mobile Device (Smartphone/Tablet)?

Yes. This is addressed in the MCU G Suite Policy Letter in Paragraph 3.D. To reiterate: this feature is completely optional but requires certain mandatory settings on the device (e.g., mandatory download of the Google Apps Device Policy application, mandatory PIN assignment of the user's choice, device auto-lock after five minutes of inactivity, etc.)

Compatible Mobile Devices at this time include those with at least the latest two versions of iOS or Android. Windows based and Blackberry devices are not supported.

20) Can I access my Google account on my personal laptop?

Yes. The system must be Windows 10 or at least the latest two versions of MacOS. Systems must also be able to support a CAC reader.

21) How many devices (Smartphone/Tablet) can I get approved to access my Google account via MDM?

The max is two per user. This means one cellphone and one tablet for example. This is access to your email account without having to use a CAC for access.

22) What is a Group, and how is it different from a Site?

Google Groups are mailing lists and online Web forums that make it easy for groups of people to communicate and collaborate over topics of common interest. There are four types and purposes of Groups.

- Email List. This type of Group is excellent for broadcast announcements, such as this one, sending links and infrequent discussions.
- Web-based Forum. Also called a Message Board, this Group works just like an email discussion, except the interface is through the browser of the website, not via email. Topics are threaded, and you can partake in multiple discussions simply by switching to a different threaded topic. This Group is great for hobbies or general-interest boards, or any group that needs a home online to have discussions, and not clutter up your email.

MARINE CORPS UNIVERSITY USER POLICY REGARDING GOOGLE SUITE (G SUITE)

- **Question & Answer Forum.** Members of these types of Groups post questions for other members to answer. Answers can be voted as the best by members, and you can up vote a post to bubble it to the top of the list. This type of Group is great for knowledge-based articles and support forums.
- **Collaborative Inbox.** This type of Group comes with a built-in workflow. You can assign topics to people, you can even take ownership of a topic to yourself. When the task or topic is done, you can mark it as Complete. This type of Group is perfect for an online Helpdesk system. It's also great for committees that usually rely on tasks by a large group of people to get things done.

Google Sites differ from groups in terms of scope and functionality. A Site is similar to the familiar SharePoint Sites that many MCU users will have experienced in the past. They combine the access management of a Group, the storage capabilities of Google Drive, as well as additional functions such as a calendar.

- 23) **Does my Google Account stay with me after I leave MCU?**
No, before you depart MCU you will be given directions on how to save your email and files for your personal storage and use.
- 24) **Is G Suite FEDRAMP approved?**
Yes, it is FEDRAMP approved.
- 25) **Can I download Apps from Google Apps Marketplace?**
This function is disabled. However, users (faculty and staff) that require additional third party apps can contact the IT Helpdesk, and the application will be vetted by the Change Control Board (CCB) for both cost and security suitability. Third-party open sourced applications are typically not approved due to security concerns.
- 26) **Is there a VTC solution that is available to use with non-CAC users?**
Yes. Google Meet allows VTC capabilities.
- 27) **Is there a bridge available for unclassified business use?**
Yes. Google Meet when used to schedule a calendar event allows conferencing with video use. Video use is not required for each event.

Marine Corps University Google Suite (G Suite) Mobile Device User Agreement Form

- I may access Marine Corps University's Google Suite (G Suite) for the purpose of "**Official Government Business Only**". As per DoDD5500.7-R, Federal Government communications systems and equipment shall be for the official use and authorized purposes only.
- I will safeguard the security of the government services on my mobile device to prevent fraudulent use by being the sole responsible user. Any lost or stolen mobile device should be reported immediately to the IT Helpdesk for suspension of access to services to prevent fraudulent access.
- I will not utilize government services on my mobile device to discuss any information that may be considered sensitive or classified as defined in SECNAV Instruction 5510.36. I am aware that it is NOT a secure transmission device. Any suspected compromise of information via this device should be reported immediately to the IT Helpdesk/ DSN 432-4866.
- I accept responsibility for the Government services attached to my personal mobile device, any actions or use of the device have been approved by me and I am sole responsible owner.
- I understand that failure to safeguard these Government services or the loss of the mobile device will result in the "wiping" of that mobile device.

**Evidence of misuse may be cause for administrative or other adverse action.
USE OF THESE SYSTEMS CONSTITUTES CONSENT TO INVESTIGATE FOR THESE
PURPOSES. For any question or clarifications, please contact IT at (703) 432-4866.**

I have read and understand my responsibilities as a Marine Corps Mobile Device and service user.

Signature _____

Printed Name/Date _____

MCU IT HelpDesk will provide a hard/soft copy of this UA for signature at the time a device is brought in for initial configuration.

August 2019



MARINE CORPS UNIVERSITY ROUTING SHEET (INTERNAL) (Rev. 07-19)

1. DATE	20201104
---------	----------

2. OPERATION CODE

X - ORIGINATOR OR OFFICE AFFIXING ROUTING SHEET	G - INFORMATION
A - APPROPRIATE ACTION	H - RETURN TO
B - GUIDANCE	I - INITIAL
C - SIGNATURE	J - DISPOSITION
D - COMMENT	K - DECISION
E - RECOMMENDATION	L - RETENTION
F - CONCURRENCE	X - ORIGINATOR
	O - (OTHER) <u>Other (define)</u>

3. Subject: MARINE CORPS UNIVERSITY USER POLICY REGARDING GOOGLE SUITE

4. NATURE OF ACTION REQUIRED	ORIGINATOR INITIALS	DUE DATE (IF ANY)
ROUTINE		
URGENT		

5. REFERENCE HELD BY (NAME, GRADE, OFFICE, PHONE)
 R.E. PITTS, Director of Administrative Services, (703) 784-6836

6. RTG	7. OPR CODE	8. ADDRESSES	9. DATE	10. INITIALS
--------	-------------	--------------	---------	--------------

5a. REFERENCE FILENAMES (IF APPLICABLE)

6. RTG	7. OPR CODE	8. ADDRESSES	9. DATE		10. INITIALS
			IN	OUT	
		PRESIDENT			
5	C,I				
4	A	CHIEF OF STAFF	11/5	11/5	[Signature]
3	A	Exec Sec to Pres/ Aide	11/06	11/06	[Signature]
2	A	SgtMaj Protocol SJA			
		VPAA			
		- Academic Support			
		- Fellowship Instructional			
		- MAGTF Group			
		- Krulak Center			
		- LCSC			
1	A	VPBA	4/Nov	4/Nov	[Signature]
	X,H	- Admin Services	11/4	11/4	[Signature]
		- Financial Management			
		- Facilities			
		- Civilian Manpower			
		VPOP			
		- IRAP			
		VPDL			
		- Dir, CDET			
		- ET			
		DIR, MCWAR			
		DIR, SAW			
		DIR, CSC			
		DIR, EWS			
		DIR, Enlisted College			
		DIR, NMMC			
		DIR, LLI			
		DIR, HD/GRC			
		DIR, CAOCL			
		DIR, IT			

11. REMARKS AND SIGNATURE

Purpose: To implement policy for the usage of Google Suite (G Suite) across Marine Corps University (MCU) and applicable stakeholders.

Recommendation: Respectfully request CG's signature.

Very respectfully,

R. E. PITTS

4/Nov - corrections.

NOV 04 2020 3679

