Acceptable Usage Policy

Acceptable Usage Policy in Global Delivery

Aim of this Policy:

Act as a reference document for the use of hardware, software and network systems by employees of all of GD, so that this policy can be understood, applied in the business, and any exceptions can be identified and raised for approval.

Security is a dynamic matter and so if the requirement changes, this document will be updated and the changes promoted in the business to achieve the necessary levels of awareness.

The Policy is intended to protect not only our business, but also our employees, by preventing mistakes and making a baseline standard approach that is common to all.

It is therefore a mandatory policy for all GD employees and they need to adhere and agree to comply with GDC derivatives of this this policy, including periodic revisions.

This Policy exists because:

- GD needs to define and apply current and effective practices to safeguard our business and the business of our customers from external and internal threat.
- Awareness of this policy in GD reduces the risk of negligence through ignorance of required practice – i.e., employees acting (often) with the best intentions, but doing something that is contrary to the rules and standards of the business.

- It is required as a part of our risk management approach – a policy exists to reduce the business risk of neglect, abuse or mistakes.

The Scope of the Policy is for all employees of GD and focuses on:

- The use of hardware and software that is provided by Fujitsu and/or connected to the Fujitsu network.
- The standards of behavior expected on corporate/enterprise systems, internet, intranet and mail systems
- The use of password security and antivirus systems that protect our IT environment
- The handling and management of data
- The human rights impacts of data privacy and data processing associated with the above points

Applicability

The policy is applicable to all employees of the Fujitsu Global Delivery Centers. For employees in GD that are also hosted by their contract of employment in a non-GDC country, they must also adhere to the terms of their local country security policy in compliance with their country laws and legislation.

Policy Statements

The Policy divides into the following domains:

- Use of Hardware
    - Use of Fujitsu-owned equipment
    - Non-Fujitsu-owned equipment
- Software
- Credentials and Passwords
- Data Handling
- Workspace Hygiene
- Antivirus and Security updates
- Email Usage
- Internet Usage
- Awareness
- Incident Reporting

Hardware - General

1. All Fujitsu IT equipment should have an identified owner assigned – i.e. a GD staff member who is responsible for the safekeeping of that equipment. An asset register must be maintained for all such equipment.
2. The (assigned) owner of the hardware is responsible for ensuring that no unauthorized software or hardware is installed on the equipment – the local ISM or IT will be able to advise on what is authorized or unauthorized.
3. GD hardware may only be used for authorized Fujitsu business purposes that is within the assigned tasks and responsibilities of the employee using the equipment
4. IT equipment should be locked or shut down when left unattended for an extended period of time
5. It is forbidden for employees to:
    a. disassemble or repair any electronic equipment within the GDC (without authorization)
    b. make changes to network safeguards and / or access these resources (including the use of software tools that facilitate circumventing these safeguards)
    c. create or use elevated access levels (perhaps provided where it is a business need) to install software; or activate or install any plug-ins that are not authorized
    d. misuse USB access (perhaps provided due to client requirements), or to copy any unauthorized: software / customer data / media content etc.
6. Disposal of Fujitsu IT equipment should only be undertaken by members of the GD technology team (or regional ITG teams). The team shall ensure that any information held on the disposed equipment is unreadable. This entails either completely deleting the information within the equipment (so that it cannot be restored) or destroying the storage device or media. In addition, appropriate degaussing methods should be used to ensure that no data is recoverable.
7. Asset disposal should be undertaken in line with the local environment and statutory requirements.

Fujitsu Provided PCs & Other Personal Equipment

1. All members of staff are responsible for the proper usage, care and cleanliness of the IT equipment they use. Line managers should ensure that all staff maintain the cleanliness of their equipment

2. GD staff should ensure their computers are fully shut down and turned off at the end of their day / shift.
3. Whenever an employee leaves the workplace, they should ensure appropriate security of IT equipment (including locking computers and saving files to appropriate data storage media, etc.)
4. Fujitsu standard screensavers (or Microsoft standard Windows screensavers) should be applied to all computers. Screensavers should have a maximum of 10 minutes before switching to screen saving mode and should require a password to unlock.
5. If an employee temporarily leaves their workstation, leaving their device behind, they are to lock the device (i.e. shutting the screen on laptops) to prevent their work being viewed or their system being accessed.
6. Loss (or theft) of portable electronic equipment must be immediately reported to the line manager and local IT, and any local security incident reporting process should be used.
7. Removable storage media by USB should be disabled by Local IT. In cases where an exception is granted to this rule Local IT is to maintain a register of granted exceptions and review these on a six-monthly basis. Such media should be password protected and encrypted.
8. Removable storage media (where allowed) and / or other portable electronic devices should never be left unattended
9. The security and safekeeping of portable and other equipment that is used outside of the GDC premises is the responsibility of the member of staff who takes that equipment outside the GDC site. As a general rule:
    a. Laptops and mobile devices may leave the site only if they have an encrypted hard drive.
    b. USB devices may not leave the site unless with permission from a manager; this would typically be for the purposes of taking presentation data to a customer site, for example. Data sets, virtual machine images, etc. may NOT leave the site.
10. If the Fujitsu assigned equipment is lost or stolen, it should be immediately reported as a security incident and all access to the equipment should be disabled. It is recommended to follow local GDC / regional procedures to report loss or theft of such equipment.
11. Portable equipment (such as notebooks and PDAs) should be carefully secured when in transit and locked away when not in use. Other recommended measures to be taken by users include:
    a. Transporting equipment in neutral cases

b. Implementing a hard disk password
c. Securing the equipment with a Kensington Lock (or similar physical lock, if provided)
d. Using screen guards to limit visibility of the display.

Non-Fujitsu-Owned Equipment

1. Personal-owned (i.e. Non-Fujitsu provided) IT equipment (hardware or software) is not to be used in GD (unless specifically approved via the Exception Management process prior to bringing the asset to the GDC premises)
2. Personal mobile phones (including those with inbuilt cameras) may be permitted within the GDC premises. In some areas within a GDC photography and videography are likely to be prohibited. This is to be clearly signed.
3. Non-Fujitsu-owned equipment is not allowed to access / connect to any part of the Fujitsu network via Bluetooth, wireless connection, external Internet or dedicated connection (unless specifically approved by a dedicated and approved visitor service or via the Exception Management process). For the avoidance of doubt, this includes all non-Fujitsu visitors (such as external auditors, contractors, customers, vendors etc.) and the person escorting the non-Fujitsu visitor will be completely responsible for ensuring that they do not allow such access and that (where required) explicit permission is granted prior to connecting to any GDC network, irrespective of any (contractual) agreements made by another country / region.
4. No external personal-owned devices (e.g. thumb drives, flash drives, and external hard disks) are allowed on GDC premises (unless approved via the Exception Management process).

Software

1. GDC employees may only load software and systems that are owned by the GDC onto their assigned IT equipment. In particular, employees may not load:
    a. Illegal software that violates copyright laws
    b. Non-approved browser software – the local ISM or IT will be able to advise on this
    c. Legal software that does not have a valid license
    d. Software that was attached to magazines or that is downloaded from the Internet (unless specifically approved by the local IT service desk)

    e. Key generators or software cracks that violate software distribution rights
    f. Freeware (source-free software agreements should be validated with CISO teams before they are used).
2. Any installation or launch of new software must be preceded by an anti-virus scan
3. Any software that is installed on IT equipment owned by Fujitsu (and which may or may not carry an associated license key) cannot be transferred to non-Fujitsu assets (such as personal electronic equipment)
4. All software installed on Fujitsu equipment must have a valid license and comply with local legislation.

Credentials and Passwords

1. All GD staff are responsible for maintaining the security of their access IDs and passwords for all systems with which they interact. This includes credentials for client and/or vendor solutions.
2. All PCs that are connected to the GDC network should have:
    a. Login / domain password
    b. Screen saver password with 10 minutes time-out.
3. Sharing of IDs and passwords is prohibited
4. Passwords should be known only to the user and cannot be shared with anyone else, regardless of the function and rank of another person
5. If there is suspicion that a password may have been disclosed internally, then the password should be changed immediately
6. If there is suspicion that a password may have been disclosed externally, then the password should be changed immediately and a local security incident created
7. Passwords should be memorable for the user and difficult to guess for outsiders. In particular, staff should avoid "simple" passwords such as: 'common passwords' (i.e. Password123) names, birth dates, car registration numbers, pet or spouse or child's name, etc. The password policy is defined in the Global Information Security Controls Framework (GISCF).
8. Passwords should be stored on approved tools that assure the security of that data. Where such tools are not provided passwords must not be stored in easily accessible locations such as: on a calendar; on the desk; on the screen; under the keyboard, etc. Passwords should not be recorded alongside login credentials.

9. Passwords should be changed on a periodic basis (as determined by the specific security needs of the system as well as any local requirements)
10. Tokens (if used) should not be shared or re-purposed for any other use.

Data Handling

1. All information / data held on IT equipment / systems that are owned by Fujitsu are deemed to be the property of Fujitsu
2. All information / data created by employees for Fujitsu projects and purposes is deemed to be the property of Fujitsu and may not be used by employees for their own purposes or shared as open source
3. For security and network maintenance purposes, authorized individuals within Fujitsu may monitor equipment, systems, logs and network traffic at any time - Fujitsu reserves the right to audit networks and systems on a periodic basis
4. Employees will not perform any disruptive or destructive activities within Fujitsu, or against any other computer system or environment.
5. No data may be shared outside Fujitsu unless the security classification level allows for the data to be shared AND appropriate (management) authorization has been provided
6. Data should not be processed or employed in ways that may negatively impact the human rights of employees, partners, customers, or end users of customers. If an employee suspects that there has been a potential negative human rights impact, they should report it in accordance with the Human Rights Policy and Human Rights Process document
7. All members of staff are responsible for ensuring that all Fujitsu / Client information is managed in accordance with the sensitivity of the information and local / client-defined security policies. In particular, the handling of information and data must be done in such a way that loss, damage, destruction and unauthorized access is prevented
8. Information sent to and received by the Fujitsu network is in the care of Fujitsu and the company reserves the right to control it. This applies to both the information and data contained in Fujitsu computers as well as any media.
9. GD staff are not allowed to post corporate or customer information on to external websites without written management authorization
10. GD staff are not allowed to post Fujitsu (or customer) intellectual property on external websites without written management authorization. This includes open-source collaboration sites and code repositories
11. All staff are responsible for ensuring compliance with relevant Data Protection; Data Privacy; and Data Residency legislation for all data processed within their

projects / activities. It is particularly important that staff can readily identify Personal Information and Sensitive Personal Information, and be alert to conditions under which this may be inadvertently disclosed, resulting in a potential data breach:

Types of Personal Information – PI (examples)	**Types of Sensitive Personal Information – SPI (examples)**
• an individual's first and last name, • an individual's Internet ID (not necessary his/her name) • e-mail address, • mailing and/or residential addresses, • telephone number, • title, • birth date, • gender, • occupation, • contact information, • credit card or bank information, • biographical information (where it is combined with information that identifies someone).	• national insurance number, • social security numbers, • race • ethnic origin • sexual orientation • political opinions • religious or philosophical beliefs • trade union memberships that contains individuals health-related records (e.g. patient records, medical photographs, diet information, hospital information records, biological traits and genetic material), • criminal records • legal investigations and proceedings, etc.

1. Any data (on IT equipment owned by Fujitsu) that is deleted or erased can be retrieved or restored at any time by Fujitsu without the prior permission of the user or notification of the user. Users will not have any privacy interest in, or expectation of any privacy concerning deleted or undeleted data and all information is any part of the computer system.
2. Employees may if they wish place personal or sensitive information on Fujitsu provided PCs. This may include pictures, bank statements, medical records, etc. However:
    a. Use of this should be limited and regarded as transient; it should not be regarded as the main or sole place where this data sits.
    b. Fujitsu reserves the right to delete the data/withdraw the device with no commitment to the employee to retain this data.
    c. The data will fall within the scope of Fujitsu monitoring technology, designed to prevent the user from attack on their endpoints.

Workplace Hygiene

1. By default GDCs will operate a clear desk policy. This means that unless approval has been given to have a non-clear desk, for example in a secured office, then:
    a. At the end of the working day, desks must be clear of business documentation that is in any way exploitable.
    b. The documentation is placed in a drawer or other holder which means that it cannot be casually viewed.
    c. Sensitive documentation should be locked away.
2. The use of printed material should be minimized. Where it is necessary to print a document then this should be appropriately handled until disposal. Sensitive printed material should be disposed of in a way which prevents recovery by any unauthorized personnel.
3. Information in notebooks, on whiteboards and flipcharts should also be managed; sensitive information on either means should be erased/shredded or collected at the end of the day.

Work from Home (Home Office enablement)

1. A secured and comfortable workplace will enable continued productivity when work is performed at home, the following are recommended guidelines for the home workplace. These are security guidelines and must also be used alongside the Occupational Health and Safety guidelines for creating a healthy and comfortable working environment.
    a. Choose your working environment to prevent other people from seeing your screen (shoulder surfing)
    b. Use secured Wired or Wi-Fi connection and avoid free or shared Wi-Fi access
2. Regularly change the default passwords for your Wi-Fi router, maintaining password complexity.
   Always store confidential information including your credentials in safe place, never write down or place these credentials in a place where other people (including your family and friends) can see this information.
3. Lock your screen when you step away from your computer, even for a short period of time. Shutdown the computer system, when not in use.
4. Keep all the Fujitsu or client provided assets in your possession secure when not in use, never leave equipment unattended.

5. Do not block/stop any security patch updates or antivirus updates, restart your system when prompted. Regularly check that anti-virus software on your PC or laptop is up to date and operating.
6. Do not install any unauthorized software or applications for personal use on company provided systems, If you need to install any software for business need then request the same through IT.
7. Never visit restricted websites, when connected from Fujitsu system or through client hardware/VPN.
8. Do not participate in chat rooms, or access any social networking sites. Never post information about Fujitsu and its clients on Internet, Blogs and Social networking sites.
9. Browsing/Downloading of text or images which contain material of a pornographic, religious or extreme political nature, or which incites violence, hatred or any illegal activity is prohibited.
10. Never use any USB media or any form of external storage on Fujitsu systems.
11. It is forbidden to disassemble or repair any Fujitsu asset (without authorization).
12. Personal-owned (i.e. Non-Fujitsu provided) IT equipment (hardware or software) is not to be used at Fujitsu or for client delivery when work is done from home.
13. Loss (or theft) of company or client equipment or data must be immediately reported.
14. Watch out for suspicious phishing emails. Never open emails from unknown parties, suspicious domains or open attachments in such emails.
15. Even though an incident may appear trivial, it may have serious legal implications. Inform your manager and/or report security incident.

Anti-Virus and Security updates

1. All IT equipment that is connected to the Fujitsu network must be equipped with up-to-date Anti-Virus software and latest security patch updates
2. This requirement for up-to-date Anti-Virus software and Security patch updates also applies to external (i.e. non-GDC) staff who are connected temporarily to the Fujitsu network
3. All GD staff should perform periodic checks to ensure that their assigned equipment has up-to-date Anti-Virus definitions and security patch updates and that the Anti-Virus software is active at all times
4. End user devices should be restarted when prompted, so that the system is updated with latest security patches

5. If a virus is detected, staff should immediately disconnect the device from the network and raise an incident with the local IT service desk and report a security incident.
6. Under no circumstances should GDC staff attempt to disable or interfere with the virus scanning software on IT equipment.
7. Other than qualified IT staff, no employee is to do virus troubleshooting or remediation on their own.

E-mail Usage

1. The Fujitsu e-mail system must not be used for political, business or commercial purposes that are not related to Fujitsu
2. The Fujitsu e-mail system must not be used to send illegal or inappropriate material. This includes using mail systems (and the Fujitsu email address) for soliciting non-company business for personal gain or profit.
3. Limited personal use of e-mail is permitted.
4. All email communication sent using the Fujitsu means should be regarded as sent by or on behalf of Fujitsu and should have a style and tone appropriate to our business
5. Sending mass / bulk e-mails is prohibited and the creation and dissemination of chain letters is forbidden. Such activities hinder the e-mail system and reduce productivity
6. All staff should use a standard Fujitsu signature format when sending official e-mails
7. Forwarding of messages from the Fujitsu e-mail platform to external (e.g. personal) e-mail addresses is prohibited (unless a written exception has been approved via the Exception Management process)
8. E-mail attachments from unknown sources should not be opened. Suspicious attachments should be deleted. Where a mailbox for the reporting of such emails by forwarding the email exists, it should be used.
9. It is forbidden to use a Fujitsu e-mail account to send files that have been obtained in violation of copyright or which are not owned by the company.
10. Inadvertent sending of emails to an incorrect, external address must be reported as a security incident in accordance with local procedures.

Internet Usage

1. Access to the Internet is provided for business purposes. Limited personal use is permitted subject to local policies.

2. No action may take place on the internet in the name of or connected with Fujitsu that exposes others, either through carelessness or intention, to material which is offensive, harassing, sexually degrading, indecent, and obscene or in poor taste. This includes information which may create an intimidating, offensive or hostile work environment
3. No action may take place on the internet in the name of or connected with Fujitsu that negatively impacts the human rights of employees, partners, customers, or end users of customers
4. Access to social media may be permitted in some GDCs. Despite the fact that the employee is using their own private identity on a non-Fujitsu platform, it is Fujitsu-owned device. Therefore no inappropriate posting behavior is allowed that is contrary to the Fujitsu Way.
5. Fujitsu's Internet access and computing resources must not be used to violate any government laws or regulations including international conventions.
6. Accessing online gambling, online gaming, standalone gaming, pornographic, illegal or other improper / inappropriate materials is prohibited. In many cases such sites may be blacklisted and access cannot be achieved. Even if access can be achieved, this does not indicate that Fujitsu allows access to the site.
7. Staff should not attempt to bypass any Fujitsu-defined website blacklisting
8. Staff should not use Fujitsu's Internet service to access materials that require large amounts of bandwidth. In particular, watching live or recorded TV / video / audio programs is prohibited (unless specifically approved via the Exception Management process – or for approved training courses)
9. Staff should avoid visiting suspicious websites in order to avoid infections from malware, worms and viruses etc.
10. Software (including screensavers) should not be downloaded from the Internet without authorization. This includes any files with extensions such as .exe, .dll etc.
11. Any materials (e.g. files and programs) that are legitimately downloaded via the Internet must be checked using up-to-date Anti-Virus software before they are first accessed / run. It is recommended that any software that is downloaded should be checked and verified by the GDC IT team before it is installed or used.
12. GD has the right to monitor Internet usage by staff
13. All Guest Internet access should be authenticated and should be person-specific, time-limited and should never be shared.

Awareness

1. It is a responsibility of all employees to have a working knowledge of this policy so that they can refer to it for occasional reference and clarification. Employees will be expected on an annual basis to indicate that they have read and will continue to adhere to this policy
2. It is the responsibility of all managers to have a working knowledge of this policy so that they can:
    a. Exemplify the policy in their working lives
    b. Be able to support others to follow the policy
    c. Be able to detect and deter breaches to the policy
    d. Be empowered to propose changes to the policy that reflect changing business requirements or security best practice.

Security Incident Reporting

1. All employees are expected to have the awareness and confidence to initiate a security incident if they identify one.
2. All managers are expected to have an awareness of the security incident reporting pathway and encourage employees to register security incidents
3. The local security incident reporting process is to be followed, if there is doubt as to the effectiveness of this or the incident is judged to be severe, then the GD CISO incident process is to be used.