

Formato para Alta de Proveedores / Acreedores / Arrendadores

Fecha:

Tipo

Obligatorio anotar la CURP

Datos Generales (Utilice mayúsculas)			
Nombre o Razón Social			
Calle	No.	Colonia	
Alcaldía o municipio		Estado	
Código postal	Teléfono 1	Teléfono 2	
	IEGG921005HVZXMS02	IEGG9210056RA	
Correo Electrónico	C.U.R.P En su caso	R.F.C.	
Documentación Antigüedad de Registro ante el SAT Cumple con la antigüedad mínima de dos años			
Si es Persona Física con: Actividad: Régimen Fiscal Cuenta Predial: ☐ ACTIVIDAD EMPRESARIAL ☐ HONORARIOS ☐ TRANSPORTISTA ☐ ARRENDAMIENTO ☐ CONTRATISTA DE PERSONAL ☐ RESICO Documentos: ☐ Identificación oficial ☐ CSF (antigüedad 2 meses) ☐ Acta constitutiva ☐ Carátula Edo Cuenta dabe (antigüedad 2 meses) ☐ Opinión de cumplimiento actual (Art 32-D CFF) ☐ Comprobante de domicilio (antigüedad 2 meses)			
Si es Persona Moral con: Actividad/Giro: Régimen Fiscal Documentos: ☐ Acta constitutiva ☐ CSF (antigüedad 2 meses) ☐ Comprobante de domicilio (antigüedad 2 meses) ☒ Carátula Edo Cuenta dabe (antigüedad 2 meses) ☐ Opinión de cumplimiento actual (Art 32-D CFF)			
Datos de cuenta y Pago			
Cuenta con Información de cuenta validada con el sello del Banco y/o Estado de cuenta bancario			
Banco		Clave del Banco (3 primeros dígitos de cuenta clabe):	
Cuenta CLABE Interbancaria (18 dígitos):	123456789098765432	Titular:	
Vía de pago		Vía:	Grupo Tesorería
Banco Pagador		Condiciones de Crédito	Cond:

Validador Tesorería

Validación Gerencia Suministros


 achavez@sisistemascontino.com.mx
 13/02/2025 12:12 pm

Indicador de Retenciones, en el caso de Personas Físicas		
☐ HONORARIOS R1 10% RETENCIÓN ISR I1 10.66% RETENCIÓN IVA	☐ ARRENDAMIENTO R3 10% RETENCIÓN ISR I2 10.66% RETENCIÓN IVA	☐ RESICO PF (ACTIVIDAD EMPRESARIAL) CE 1.25% RETENCIÓN IVA
☐ TRANSPORTISTA I5 4% RETENCIÓN IVA	☐ RESICO PF (ARRENDAMIENTO) CA 1.25% RETENCIÓN ISR I2 10.66% RETENCIÓN IVA	☐ RESICO PF (HONORARIOS) CH 1.25% RETENCIÓN ISR I1 10.66% RETENCIÓN IVA

Observaciones

ESCRIBIR EN LOS SIGUIENTES RECUADROS LOS DATOS DEL RESPONSABLE DE SUBIR LAS FACTURAS AL PORTAL PORAPP PARA PAGO:

Nombre completo:

Correo electrónico:

Número telefónico:

Solicitante

Director de área solicitante

€

Administración de Datos Maestros

—



MÉXICO

INSTITUTO NACIONAL ELECTORAL
CREDENCIAL PARA VOTAR



NOMBRE
IXTEPAN
GOMEZ
GUSTAVO ADOLFO

SEXO H

DOMICILIO
C MAGDALENA MARQUEZ 101
FRACC VILLA RICA 91810
VERACRUZ, VER.

CLAVE DE ELECTOR IXGMGS92100530H100

CURP
IEGG921005HVZXMS02

AÑO DE REGISTRO
2010 03

FECHA DE NACIMIENTO
05/10/1992

SECCIÓN
4218

VIGENCIA
2023 - 2033



Cef¹⁸

RFC: IEGG9210056RA
Nombre: GUSTAVO ADOLFO IXTEPAN GOMEZ

Hoja 1 de 1

Tipo de declaración:	Normal	Ejercicio:	2022
Período de la declaración:	Del Ejercicio	Medio de presentación:	Internet
Fecha y hora de presentación:	03/04/2023 11:11		
Número de operación:	231300003747		

Impuestos que declara:

Concepto de pago 1:	ISR PERSONAS FÍSICAS
A favor:	468
Cantidad a cargo:	0
Cantidad a pagar:	0

INGRESOS QUE DECLARA:

Sueldos, salarios y asimilados

Es recomendable verificar que el importe calculado de la parte actualizada esté correcto, en virtud de que puede haber cambiado el índice nacional de precios al consumidor y el cálculo debe estar basado en el último publicado.

Los datos personales son incorporados y protegidos en los sistemas del SAT, de conformidad con las disposiciones legales en la materia.

Para modificar o corregir datos personales visita sat.gob.mx.

Este acuse es emitido sin prejuzgar la veracidad de los datos asentados ni el cumplimiento dentro de los plazos establecidos. Quedan a salvo las facultades de revisión de la autoridad fiscal.

Sello digital :

bC8AzgJ4eKS3CG/ 3063Js0zi THACCHFFI HGx0o13mt Nt / 1QuOUadxF8eP4xdHppD2Pt I EH2e2pB3/ wf I JCC8DLpPN+hxnabXn/ Jj
hrXaW6RDJt mj Qp8qHpCQI AL3dVW 4FwS3YBc2GQ65aTHEt FUOr h1U5f cgF9FMLj f j dPZZd+yBl svwmrdoQHUL8nk7Qp99Yk7ar nK
BC8kj 1i PZ6W r j RU9VWn0z8E+Fnwj pQ4j t C4af a8j ygSebl 0TYBuLNeCl wMp2H6DsBsZi W 77PxnQqbPoFKVGORUL8Rj UPsNyZ9E
5UHr xnLFI GcMyvS4/ DdZO4/ 8oN9QueQMpDi R6z3L4g==



Comisión Federal de Electricidad®

CFE Suministrador de Servicios Básicos
Río Ródano No. 14, colonia Cuauhtémoc,
Alcaldía Cuauhtémoc, Código Postal 06500,
Ciudad de México. RFC: CSS160330CP7

SANCHEZ MALD REYNA Y

EMILIANO ZAPATA M16 L3 PA
PLAN DE AYALA Y 10 DE ABRIL
EMILIANO ZAPATA FRAC. POPULC.P.04919
COYOACAN,CDMX

NO. DE SERVICIO:968080302635

RMU:04910 08-03-19 XAXX-010101 006 CFE

CUENTA:10DN70B871010250

LÍMITE DE PAGO:21 DIC 2024

CORTE A PARTIR:22 DIC 2024

TARIFA:01**NO. MEDIDOR:**D274940

MULTIPLICADOR:1

NO HILOS:1

PERIODO FACTURADO:04 OCT 24-05 DIC 24

TOTAL A PAGAR:

\$61

(SESENTA Y UN PESOS M.N.)



Concepto	Lectura actual		Lectura anterior		Total periodo	Precio (MXN)	Subtotal (MXN)
	Medida ☒ Estimada ☐		Medida ☒ Estimada ☐				
Energía (kWh)	8,835		8,831		4		
Basico					4	1.055	4.22
Este gráfico refleja tu nivel de consumo. A menor uso, mayor apoyo.							
Subtotal							

Costos de la energía en el Mercado Eléctrico Mayorista					Desglose del importe a pagar	
Concepto	\$	\$/kW	\$/kWh	Importe (MXN)	Concepto	Importe (MXN)
Suministro	0.00	0.00	0.00	0.00	Energía	52.75
Distribución	0.00	0.00	0.00	0.00	IVA 16%	8.44
Transmisión	0.00	0.00	0.00	0.00	Fac. del Periodo	61.19
CENACE	0.00	0.00	0.00	0.00	Total	61.19
Energía	0.00	0.00	0.00	0.00		
Capacidad	0.00	0.00	0.00	0.00		
SCnMEM(1)	0.00	0.00	0.00	0.00		

Fecha, hora y lugar de impresión:06/02/2025 11:35:33hrsCalle Francisco Gotia11Barrio de San PedroXochimilcoCiudad de MéxicoCiudad de MéxicoMéxico16090

(1) SCnMEM: Costos relacionados con los servicios del Mercado. (2) DAP: Derecho al Alumbrado Público. (3) Cargos o créditos: Diversos conceptos que se pueden incluir en el aviso recibo relacionados con el suministro.

CFE **contigo**



04910 08-03-19 XAXX-010101 006 CFE
01 968080302635 241221 000000061 0



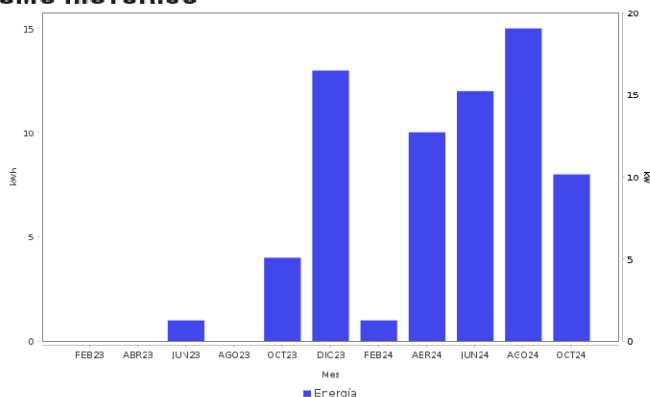
\$61

(SESENTA Y UN PESOS M.N.)

10DN70B871010250Repartir

CONSUMO HISTÓRICO

Periodo	kWh	Importe	Pagos	Pendientes de Pago
del 05 AGO 24 al 04 OCT 24	8	\$61.00	\$61.00	
del 05 JUN 24 al 05 AGO 24	15	\$60.00	\$60.00	
del 04 ABR 24 al 05 JUN 24	12	\$60.00	\$60.00	
del 02 FEB 24 al 04 ABR 24	10	\$59.00	\$59.00	
del 05 DIC 23 al 02 FEB 24	1	\$59.00	\$59.00	
del 05 OCT 23 al 05 DIC 23	13	\$58.00	\$58.00	
del 04 AGO 23 al 05 OCT 23	4	\$58.00	\$58.00	
del 06 JUN 23 al 04 AGO 23	0	\$57.00	\$57.00	
del 04 ABR 23 al 06 JUN 23	1	\$56.00	\$56.00	
del 03 FEB 23 al 04 ABR 23	0	\$56.00	\$56.00	
del 06 DIC 22 al 03 FEB 23	0	\$54.00	\$54.00	



AHORRO DE ENERGÍA AIRE ACONDICIONADO

- La temperatura de confort óptima se sitúa entre los **24 y 26 °C**, mantener la temperatura por debajo de los 20 °C causa un mayor trabajo del compresor, lo que supone un mayor consumo de energía.

Asimismo, se recomienda apagar el aire acondicionado al salir del recinto durante tiempo prolongado (más de 30 minutos).

Datos Fiscales del Receptor Cadena Original Este documento es una representación impresa de un CFDI PPD
 RFC: Razón Social: Régimen Fiscal: 000 Uso CFDI: CP: 00000 AC:Folio: 000275011379 Folio Fiscal: N. Certificado del SAT: No. certificado del CSD: Fecha y hora de certificación: Unidad de medida: kWh
 |||||



Instancias y recursos a disposición de los usuarios para atender quejas:



Suministrador de Servicios Básicos



¡AVISO IMPORTANTE!

Ahorra consumo de energía eléctrica, tu ahorro contribuye a la protección del medio ambiente. Nuestro compromiso es seguir conectados contigo.

Corte a partir del 22 DIC 2024.

Usted consume menos de 50 kWh al bimestre.

Le invitamos a que se registre en nuestro portal y disfrute de la comodidad de nuestros servicios en línea.

Conoce los servicios de los diferentes suministradores: <http://usuariocalificado.cre.gob.mx/UsuarioCalificado/ListadoSuministrador>

TAMBIÉN PUEDES PAGAR TU RECIBO EN:



Banco del Bienestar, Bancomer, Inbursa, Santander, Banamex, Banjercito, Scotiabank, HSBC, CIBanco, Afirme, Multiva, Banco del Bajío, Banco Azteca, OXXO, Coppel.

Son más de 100,000 establecimientos autorizados, consulta el portal cfe.mx en la sección medios de pago.

HP Support: Cybersecurity Best Practices

November 2024

Global Training



Welcome to the training for HP Support: Cybersecurity Best Practices!

We will look at an introduction to cybersecurity, how to identify cyber threats, and how to safely support a customer during a remote consultation or onsite intervention. We'll also discuss how to deal with cybersecurity incidents and how to safely use USB devices when servicing a PC. Lastly, we will look at the proper escalation process to follow when a possible cyber attack is suspected, or a system has been compromised.

What's this course about?

There are four modules:

- Module 1—Importance of cybersecurity
- Module 2—Best practices for onsite support
- Module 3—Best practices for remote support
- Module 4—Escalating cybersecurity incidents



There are four parts to this training.

After completing this course, you will be able to:

- Recognize the importance of cybersecurity
- Specify best practices for onsite support
- Specify best practices for remote customer support
- Determine the escalation process for handling cybersecurity incidents

Importance of cybersecurity



3 HP Private, Confidential for

Module 1: Importance of cybersecurity

What will I learn?

After you complete this module, you should be able to:

- Recognize the importance of cybersecurity
- Enhance the awareness of cybersecurity

Source:
4 HP Private, Confidential for Internal Use Only



In this module, we will look at why it is important to safeguard your HP service PC and the customer's PC from malicious cyber attacks.

After completing this module, you should be able to:

- Recognize the importance of cybersecurity
- Enhance the awareness of cybersecurity

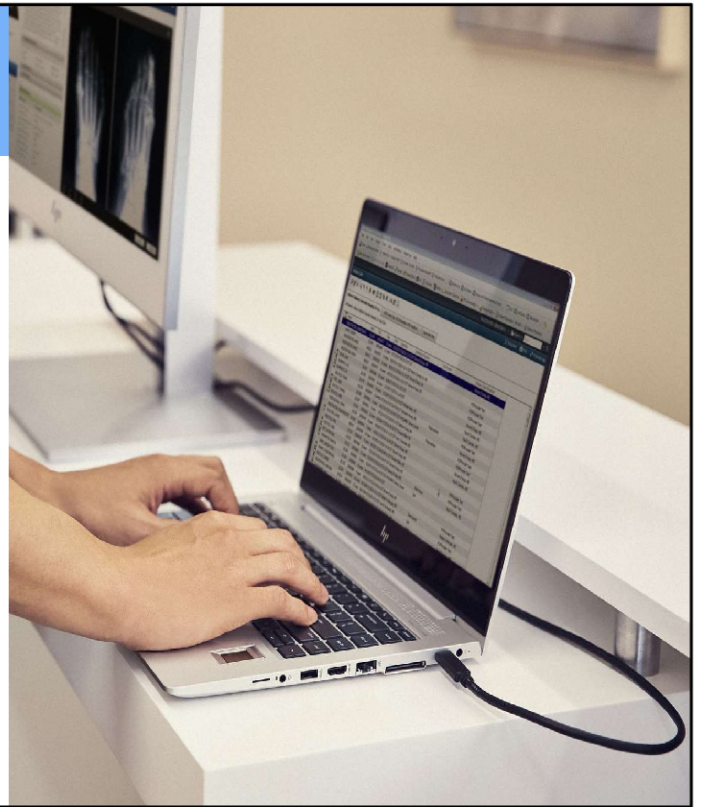
Importance of cybersecurity

What is cybersecurity?

- Safe-guard HP systems and devices
- Security features:
 - Monitor PCs and systems
 - Effective response
- Agent responsibilities:
 - Recognize cyber threats
 - Understand the customer's security practices
 - Take proper action

Source:

5 HP Private, Confidential for Internal Use Only



Cybersecurity encompasses the safety measures HP employs to protect electronic devices, data, programs, and internet-connected support systems from cyber attacks. HP's cybersecurity framework uses advanced security features to monitor PCs and systems to effectively respond to identified security risks.

As an agent that services customer PCs, it is your responsibility to recognize cybersecurity threats and respond appropriately to incidents when supporting customers. It's also a good idea to understand the customer's security practices and make sure that you are abiding by them.

Importance of cybersecurity

Why is cybersecurity important?

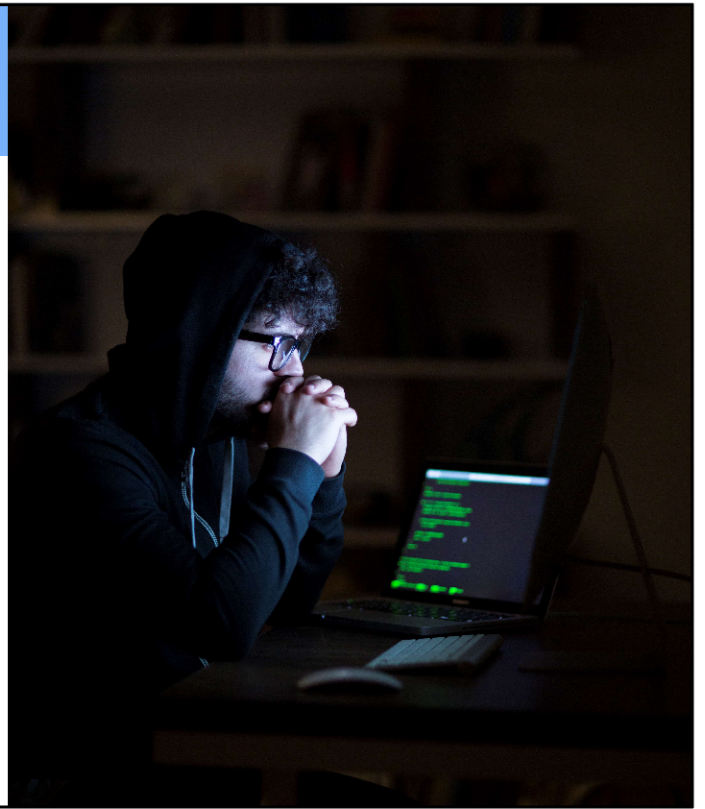
Cybercriminals

- Steal data
- Sabotage systems
- Disrupt operations

Be vigilant!

Source:

6 HP Private, Confidential for Internal Use Only



Cybercriminals target customers and companies to steal data, sabotage systems, and disrupt local and international operations. Identifying and managing cybersecurity risks during customer support are important because you want to be sure that customers' computer systems remain secure and protected from unauthorized access, data breaches, and infections by electronic viruses. Additionally, safeguarding against cyber crimes is vital for protecting HP's integrity and security.

Importance of cybersecurity

What are cybersecurity threats?

Cyber programs used to access and harm users' computers

Common cybersecurity threats include:

- Phishing/Social Engineering
- Spoofing
- Malware
- Denial-of-Service (DoS) attacks

Important! The [HP Cybersecurity Best Practices](#) website
(Note: HP internal use only)

Source:
7 HP Private, Confidential for Internal Use Only



Cybercriminals often use common cyber programs to access and harm the computers of unsuspecting users. These cyber programs, also called cybersecurity threats, can damage customers' PCs or even an HP support portal!

Common cybersecurity threats that you should be aware of include:

- **Phishing/Social Engineering:** These attacks use email, text messages, or fake websites to trick users into revealing sensitive information, such as login credentials or banking details.
- **Spoofing:** Spoofing attacks impersonate legitimate sources, like email addresses or websites to deceive users into providing sensitive information.
- **Malware:** Malware encompasses a range of threats like ransomware, trojans, viruses, and spyware designed to harm computers, networks, or servers by altering, stealing, or destroying data. Ransomware, for example, encrypts computer data and demands a ransom for its release.
- **Denial-of-Service (DoS) attacks:** In a DoS attack, cybercriminals flood a system or network with excessive traffic, causing it to become unavailable to legitimate users.

For more information on additional types of cybersecurity threats, please visit the HP cybersecurity website "HP Cybersecurity Best Practices". Please note that this site is for HP internal use only.

Importance of cybersecurity

Impacts of cyber-attacks for customers

- Identity theft
- Data loss
- Data encryption
- Financial loss
- Reputational damage

Impacts of cyber-attacks for HP

- Lack of customer trust
- Devalues HP's stance as the world's most secure PC and print manufacturer



Cybersecurity threats can have a negative impact on both customers and companies like HP.

For customers, a cybersecurity threat can result in identity theft, data loss, data encryption, and financial loss.

For companies like HP, cybersecurity incidents – especially those occurring during customer service interactions – can lead to severe consequences, including loss of customer trust, reputational damage, and a devaluation of HP's standing as the world's most secure PC and print manufacturer.

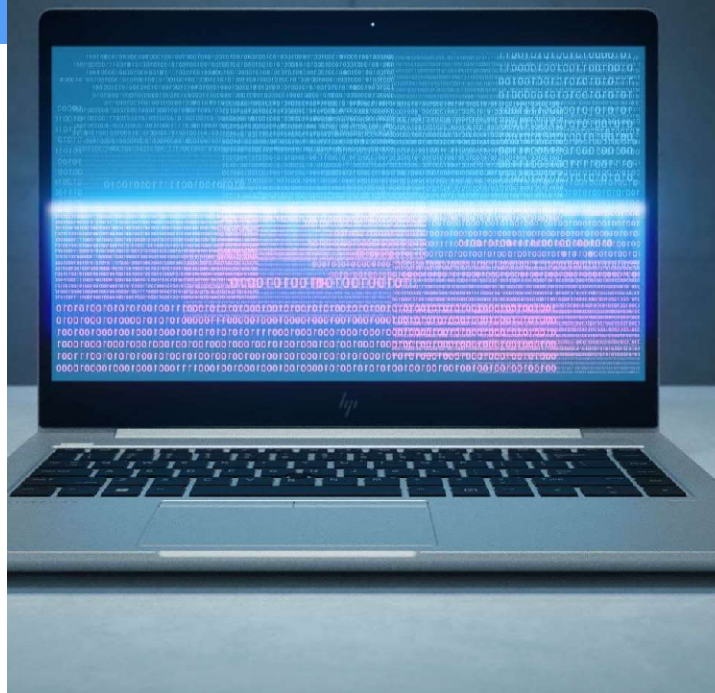
Importance of cybersecurity

Cybersecurity risks during support

Be aware of cybersecurity risks

Types of customer support:

- Remote support
- Onsite support



9 HP Private, Confidential for Internal Use Only

When you service a customer's PC, they entrust you with a device that may contain personal information, sensitive files, and business and intellectual property. Any cybersecurity breach could expose the PC to hacking and cyber theft. It's important to be aware of the security risks involved when supporting customers, ensuring that both your service PC and service USB are virus-free to avoid compromising the customer's system.

Customers have access to two types of support based on their warranty, location, and whether their device is within warranty. Remote support is available to all customers, while onsite support depends on the warranty type and status.

As a service agent, you should be aware of the cyber security risks involved when supporting customers. Next, we will cover best practices for ensuring cybersecurity in both onsite and remote scenarios.

Try It!

What are the types of cyber attacks that could result in identity theft?

Select all that apply.

- A. Malware
- B. Denial-of-Service (DoS) attacks
- C. Spoofing
- D. Phishing

Source:

10 HP Private, Confidential for Internal Use Only



What are the types of cyber attacks that could result in identity theft?
Select all that apply.

Try It!

What are the types of cyber attacks that could result in identity theft?

Select all that apply.

- A. **Malware**
- B. Denial-of-Service (DoS) attacks
- C. **Spoofing**
- D. **Phishing**

Source:
11 HP Private, Confidential for Internal Use Only



The correct answers are A, C and D.

Best practices for onsite support



12 HP Private, Confidential for

Module 2: Best practices for onsite support

What will I learn?

After you complete this module, you should be able to:

- Specify the required preparations before onsite visits
- Specify best practices when providing onsite support
- Specify the necessary tasks after providing onsite support

Source:
13 HP Private, Confidential for Internal Use Only



In this module, we will look at cybersecurity threats you should be aware of when supporting customers onsite.

After you complete this module, you should be able to:

- Specify the required preparations before onsite visits
- Specify best practices when providing onsite support
- Specify the necessary tasks after providing onsite support

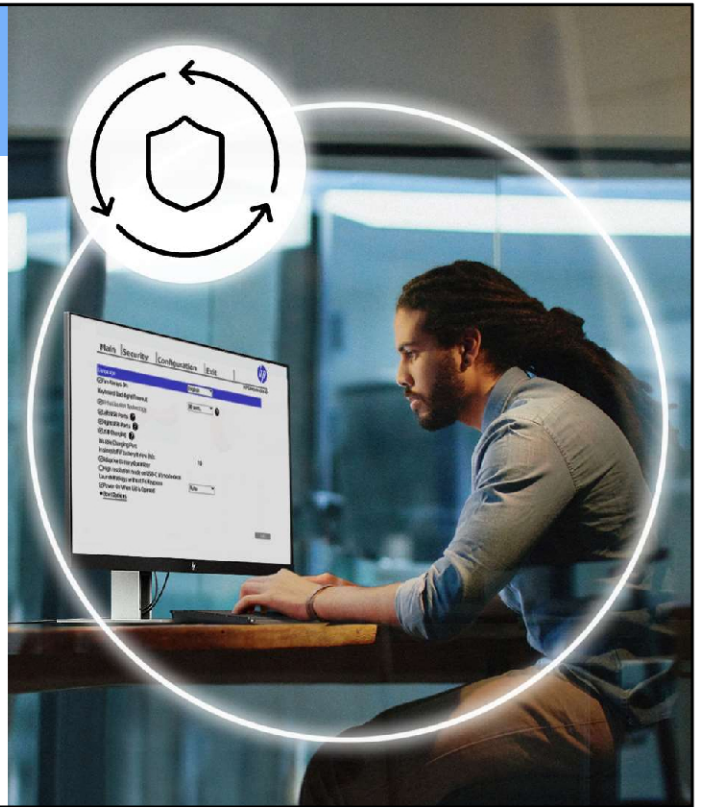
Best practices for onsite support

Before an onsite visit

- Review cybersecurity protocols
 - Use the HP Product Security policy
 - To address vulnerabilities and mitigate risks, view:
 - [Coordinated Vulnerability Disclosure](#) policy
 - [Security Bulletins](#)
- Scan your service notebook and USB drive

Note: Do not use your personal notebooks or USB drives for onsite support.
- Download required software and firmware
- Encrypt USB drives
- Check that customer has a PC, USB drive, and internet connection

Source:
14 HP Private, Confidential for Internal Use Only



Always be mindful of the cybersecurity risks that could affect a customer's PC during onsite repairs. Before providing onsite support, ensure that you

Review the processes and protocols outlined in the HP Product Security policy. For information on how to address cybersecurity vulnerabilities and mitigate potential risks as quickly as possible, you should review these resources:

- Coordinated Vulnerability Disclosure policy
- Security Bulletins for the latest security updates

Scan your service notebook and USB drives to ensure that they are virus-free and safe to use, and check that the antivirus software on your service notebook is up-to-date. Note: Do not use your personal notebook or USB drives to provide onsite support.

Download any required software and firmware to your service USB drive.

Encrypt your service USB drives to prevent unauthorized access to the data stored on it. We'll look at how to encrypt your service USB drives in the next slide.

Check that the customer has a working PC, USB flash drive, and internet connection for downloads and installations.

Best practices for onsite support

Encrypting USB drives

Why encrypt?

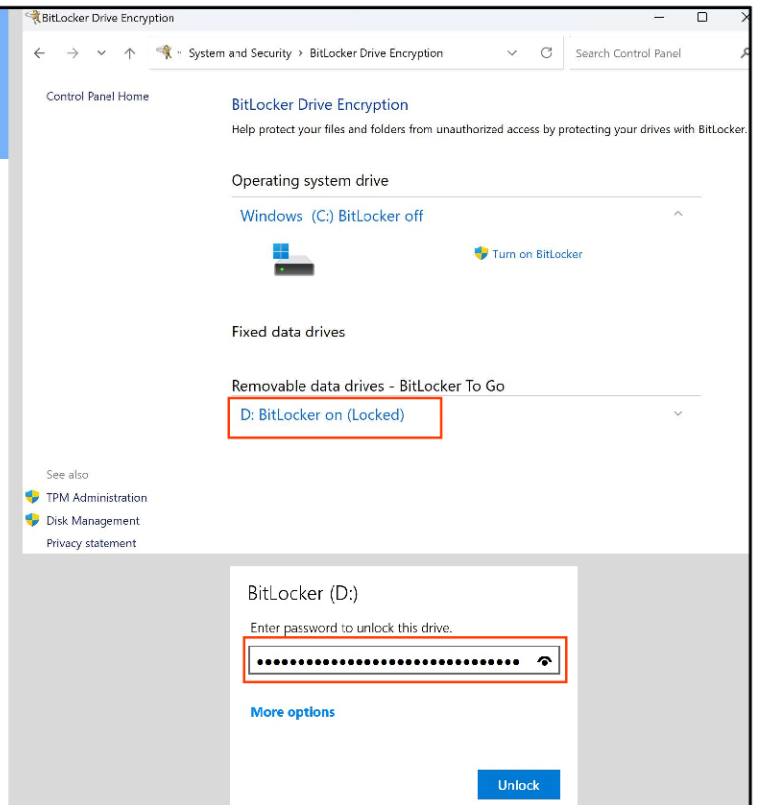
- Saved data is vulnerable
- Hackers can access content

What to do?

- Use BitLocker to encrypt data on the USB drive
 - Password is required to unlock the drive

Note: Do not encrypt the DMIFIT tool.

Source:
15 HP Private, Confidential for Internal Use Only



To minimize cybersecurity risks, it is important to encrypt all USB drives used with HP devices and customer devices.

Without encryption, data saved on your service USB drive will be vulnerable as hackers can bypass the antivirus software, firewall, or other security controls to access the device contents.

To encrypt data on a USB drive, insert the USB drive into a USB port on your Windows device. Open File Explorer, right-click the USB drive, select BitLocker, and follow the on-screen prompts. Once encrypted with BitLocker, a password is required to access any data on the drive.

One thing to note is some utilities, like the DMIFIT tool, may not function on an encrypted USB.

Best practices for onsite support

During an onsite visit

- Ensure customer's PC and USB drive is virus-free
 - Use the service PC and VPN to connect to HP SharePoint sites and download resources
 - Use the service PC for internet connectivity
 - Use dedicated USB drives for specific tasks
 - Scan service USB drives before inserting into customer's PC
 - Inform customers to report issues via:
 - [HP online submission form](#)
 - Email at [HP Security Alert](#)
- Note: Customer should encrypt sensitive data using the [HP Product Security Response Team's \(PSRT\) PGP](#)

Source:

16 HP Private, Confidential for Internal Use Only



During an onsite visit, it is your responsibility to manage both your service devices carefully to prevent them from being exposed to cyber threats.

Make sure that the customer's PC is virus-free if it will be used to connect to HP support sites. Also check that the customer's USB drive is virus-free and only use your service USB drive if you suspect the customer's USB drive is not clean, or there is no other USB drive available.

Use the service PC and a virtual private network (or VPN) if you need to access the HP SharePoint sites or HP network to download resources, like drivers software, to fix the customer's PC. This remote access via VPN enables secure access to HP network resources from different locations, allowing you to download necessary data to your service PC and transfer it to the service USB. Do not use the customer's PC to access the HP network. Only the service PC with VPN should be used for this purpose.

Use the service notebook if there is no available internet connection.

Use dedicated USB drives for specific tasks, such as branding or transferring BIOS and files to a customer's computer. Do not use personal USB drives for work, nor USB drives from unknown sources.

Always virus-scan USB drives before inserting them into a customer's computer.

If a customer asks for advice on managing a cybersecurity issue on their HP product, inform them that they can report security vulnerabilities via the:

- HP online submission form, or
- Via Email @HP Security Alert

For reports containing sensitive data, customers should use the HP Product Security Response Team's (PSRT) PGP key to encrypt the content.

Best practices for onsite support

After an onsite visit, you should:

- Run antivirus scans on service PC and USB
- Escalate any cybersecurity issues

After an onsite visit, you should not:

- Bring an infected service PC into HP
- Connect an infected service PC to HP sharepoints

Source:

17 HP Private, Confidential for Internal Use Only



After you've completed an onsite visit, perform the following tasks to protect HP from cybersecurity risks, and to address potential exposure to cyber threats on your service USB or service PC.

Dos:

- Run antivirus scans on both the service PC and USB to ensure they are virus-free
- Escalate any cybersecurity issues, if required

Don'ts:

- Do not bring any infected devices (service PC, USB, etc.) into the HP or customer environments - clean them first!
- Do not connect an infected service PC to HP sharepoints

Best practices for remote support



18 HP Private, Confidential for

Module 3: Best practices for remote support

What will I learn?

After you complete this module, you should be able to recognize cybersecurity risks during remote support

Source:
19 HP Private, Confidential for Internal Use Only



Understanding the importance of protecting customer data is important when providing support.

By the end of this module, you will be able to identify potential cybersecurity risks when supporting customers remotely.

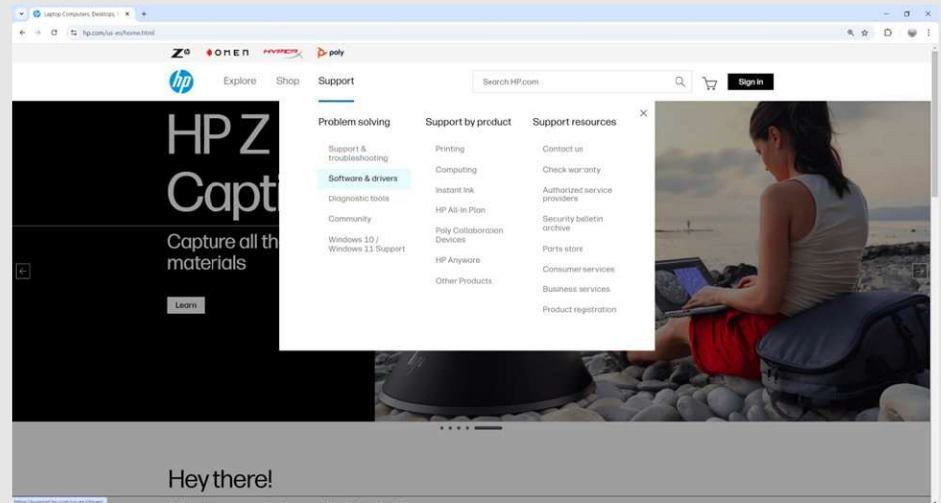
Best practices for remote support

Only download driver and BIOS updates from www.HP.com

- HP has multiple type of software that can be downloaded for devices
- Printer drivers
- Printer management software
- BIOS updates

For details on how to download, install and update drivers and software from HP.com, visit:

- [HP Printer Software Download: How To Download And Install The Latest Version](#)



20 HP Private, Confidential for Internal Use Only

When customers contact you about a hardware failure or software issue, these problems can often be resolved by guiding them to install the latest driver for the malfunctioning part, or by updating the system's BIOS.

It is important to advise customers to always download BIOS and drivers exclusively from the HP Customer Support website for the specific computer model only. Sometimes drivers are available for a similar system or hardware product on suspicious online sites. It is recommended to not install drivers from non-HP sites as these drivers very often have some malware or computer viruses embedded which could lead to ransomware attacks on the system.

Best practices for remote support

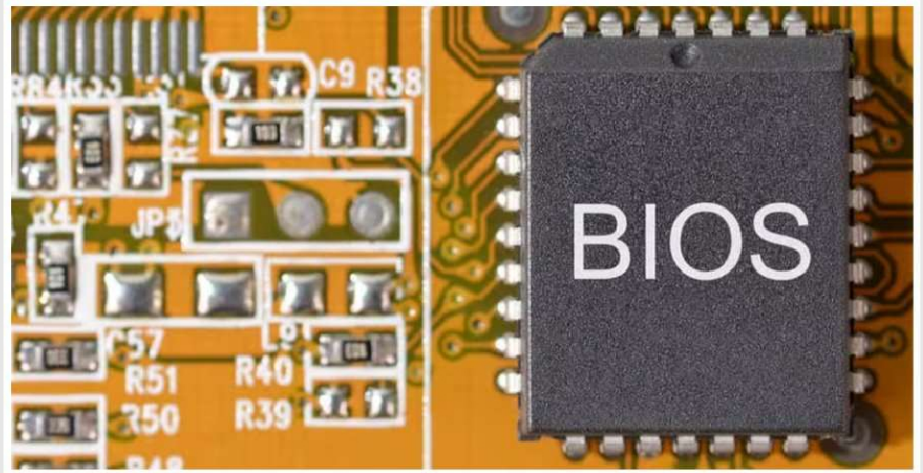
How to update BIOS software

Use the latest BIOS updates for security and performance

Download and install a PC BIOS update from website:

How to Update BIOS Software on Windows PCs

<https://www.hp.com/us-en/shop/tech-takes/how-to-update-bios-software>



21 HP Private, Confidential for Internal Use Only



To keep computers secure and performing optimally, advise customers to visit the following HP website for detailed instructions on how to download and install the latest BIOS update:

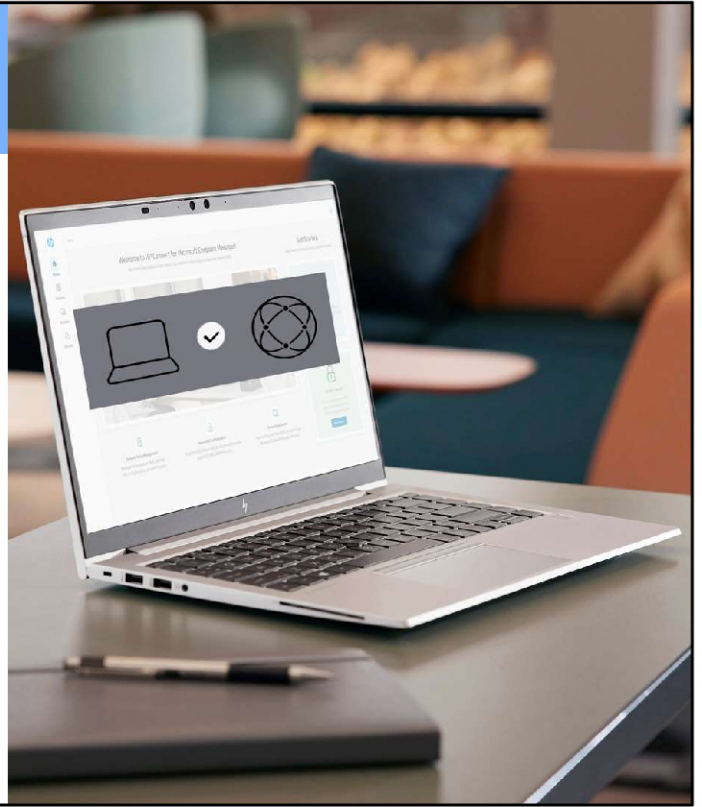
<https://www.hp.com/us-en/shop/tech-takes/how-to-update-bios-software>.

Best practices for remote support

Remote interaction

Use a VPN to connect remotely to customer PC

Source:
22 HP Private, Confidential for Internal Use Only



If installing the latest drivers and BIOS updates does not resolve the customer's issue and you need to access their PC remotely for online support, make sure to use a virtual private network (VPN) to do so. VPNs encrypt data moving between remote devices and the network, thereby enhancing security for HP and the customer PC.

Escalating cybersecurity incidents



23 HP Private, Confidential for

Module 4: Escalating cybersecurity incidents

What will I learn?

After you complete this module, you should be able to determine the escalation process for handling a cybersecurity incident involving a PC or printer

Source:
24 HP Private, Confidential for Internal Use Only



If you encounter a cybersecurity threat on your HP service PC or a customer PC, you must escalate the incident to HP Cybersecurity.

After you complete this module, you will be able to determine the escalation process for handling a cybersecurity incident involving an HP PC or printer.

Printers and personal systems

How to escalate a cybersecurity incident

- Escalate the incident to your PSDM
- PSDM to create a ticket
- Paths for incident escalation:
 - Partners to contact their PSDM
 - CEs to contact their HP District Manager
 - Partner CEs to contact their HP partner managers
- Incidents reported to the HP Cybersecurity response team

Source:
25 HP Private, Confidential for Internal Use Only



When you identify a possible cybersecurity issue on a customer's HP printer or PC, you need to escalate the issue to the Partner Service Delivery Manager (PSDM), who will create a ticket for cybersecurity incident.

Partners and Customer Engineers (CEs) should follow these escalation paths:

- Partners should contact their PSDM
- CEs should contact their HP District Managers (HPDM)
- Partner CEs should contact their HP partner managers

All escalation paths should result in the reporting of the incidents to the HP Cybersecurity response team.

Thank you



Thank you.



MÉXICO

INSTITUTO NACIONAL ELECTORAL
CREDENCIAL PARA VOTAR



NOMBRE
IXTEPAN
GOMEZ
GUSTAVO ADOLFO

SEXO H

DOMICILIO
C MAGDALENA MARQUEZ 101
FRACC VILLA RICA 91810
VERACRUZ, VER.

CLAVE DE ELECTOR IXGMGS92100530H100

CURP
IEGG921005HVZXMS02

AÑO DE REGISTRO
2010 03

FECHA DE NACIMIENTO
05/10/1992

SECCIÓN
4218

VIGENCIA
2023 - 2033



Cef¹⁸



ELECCIONES FEDERALES

LOCALES Y EXTRAORDINARIAS



8002171

M^{ra} Elena Cornejo Espinosa

MARIA ELENA CORNEJO ESPINOSA
ENCARGADA DEL DESPACHO DE
LA SECRETARIA SUBSISTIVA DEL
INSTITUTO NACIONAL ELECTORAL

IDMEX2552389547<<4218087159645
9210055H3312315MEX<03<<33323<5
IXTEPAN<GOMEZ<<GUSTAVO<ADOLFO<

Aguascalientes	AS
Baja California	BC
Baja California Sur	BS
Campeche	CC
Coahuila de Zaragoza	CL
Colima	CM
Chiapas	CS
Chihuahua	CH
Ciudad de México	CDMX
Durango	DG
Guanajuato	GT
Guerrero	GR
Hidalgo	HG
Jalisco	JC
México	MC
Michoacán de Ocampo	MN
Morelos	MS
Nayarit	NT
Nuevo León	NL
Oaxaca	OC
Puebla	PL

Querétaro	QT
Quintana Roo	QR
San Luis Potosí	SP
Sinaloa	SL
Sonora	SR
Tabasco	TC
Tamaulipas	TS
Tlaxcala	TL
Veracruz	VZ
Yucatán	YN
Zacatecas	ZS
Nacido en el Extranjero	NE

6S, 6C, 5L, 3T, 3R, 2G, 2N, Z, E, X, P, H, M

S C L T R G N Z E X P H M

C E G H L M N P R S T X Z

[CEGHLMNPRSTXZ]

ID DEL DOCUMENTO: f3fccf55-7413-422c-99e9-126eaa7adf6.
NOMBRE
FECHA DE CREACIÓN 13-02-2025 12:11 pm
FOLIO MUMONTEPIO_AP04



Ver este documento en
CONTISIGN



Validar este u otro
documento

Persona que firma: Ángel Chavez
Correo electrónico: achavez@sistemascontino.com.mx
Dirección IP: 187.251.212.179
Fecha y hora de firma: 13-02-2025 12:12 pm Hora CDMX
Firma interna: 4mz4cSz8UZbIHs+wtvHKocyWfNM5FTm5lhWpuZIPJw8=