bookwiz
bring your life back into balance

ATO Lodgement Dates

These dates are from the ATO website and do not take into account possible extensions.
You remain responsible for ensuring that the necessary information is with us in time.

BAS/IAS Monthly Lodgement

November Activity Statement: 21st December, 2016 is the final date for lodgement and payment.

December Activity Statement: 21st January, 2017 is the final date for lodgement and payment.

2nd Quarter of FY 2017: BAS Lodgement – October to December 2016 (including PAYGI)

28th February 2017 is the final date for lodgement & payment

When a due date falls on a Saturday, Sunday or Public Holiday, you can lodge or pay on the next business day.
A public holiday is a day that is a public holiday for the whole of any state or territory in Australia

Please Note: Due date for Super Guarantee Contributions, for:

2nd Quarter of FY 2017, October to December 2016 - contributions to be made **to the fund** by 28th January 2017

Cyber Security of your Software

Backup of Computers and all Data

Backup is essential. Offsite, remote or cloud backup is the best option; you can “set and forget”, and it then happens automatically in the background.

Alternatively use an external drive and schedule regular backups, e.g. at the end of each work day.

Electronic Document Storage

Electronic storage of business records is allowable but you must have a secure process for backup and access in place. You must keep records of who has access and at what level. As these are your legal business records, care must be taken to maintain integrity and security of these records.

Passwords and User Access

Keep a log of who has access to what application. It is easy to forget who you have given access to for what software or applications. Make sure that when a staff member leaves, you also rescind their access to your software, banking, supplier and customer information and any other applications.

Regularly update and change your passwords. You should be using a secure password generator as well and consider using a password vault or manager such as 1Password or Last Pass to keep all your logins secure. Using a password vault means you only have to remember one password - you can then log in to all your other applications from within the vault.

Cyber and Email Security

At a minimum, you should have anti-malware and anti-virus protection on all devices. For best security, you should also have an email security gateway to act as an intermediary between the internet and your email inbox. This will reduce the amount of spam emails you receive. We recommend Secure ISS for all of these solutions.

Settings and Preferences

All of your devices and all applications and programs that you use have setting and preferences that you are able to customise for the greatest level of security. We recommend you always choose the highest level of security available.

Accounting Software

Regularly check the registered users of your accounting software and their level of access, to ensure there have not been any unauthorised users added to your account. Conduct audits of the system to look for duplicated bank accounts, supplier names you are not familiar with or any unusual activity. If you use online payment gateways to send or receive payments, check their security options.

Two Factor Authentication (2FA)

2FA adds a second level of authentication to a login process. Entering a username and password is considered a single-factor authentication. 2FA requires the user to have more credentials to log into an account. It has been around for many years and we are used to using it for banking and interacting with government departments.

For any service or application that offers two-factor authentication, enable it right now for every sign-in. If you are using software or other applications that do not currently offer two-step verification, get on their forums or feedback areas to request this feature.

Scamwatch

Scammers are becoming increasingly sophisticated and creative. Always be on the lookout for potential scams. Sign up for Scamwatch newsletters to stay abreast of current scams. Also check the ATO scam webpage for information relating to tax scams.

Identity of Software Company Representatives

If a representative of your software company contacts you, always check their identity and ask for a means of verifying them. If you have a dedicated account manager, always check with them if it is feasible to do so, or even raise all issues through them if possible. Be particularly watchful if a software rep wants to access your file. If they take over your computer through Team Viewer or similar, always watch what they are doing and if you are suspicious, end the session immediately. Do not leave the computer while they are working on it. Make sure they are only accessing areas that are relevant to that software company.

Legitimacy of Cold Calls and Emails

If you have not placed a call, logged an issue with their online system or otherwise initiated contact, be suspicious of anyone calling you claiming to be a representative from a company, even if it is one you regularly deal with, and even if their claim sounds plausible.

If you are interested in what they are offering or asking, always ask for their identification and a means of verifying that they work for the company they claim to be working for. Do not give out personal information unless you are sure of who you are speaking to.

If you receive emails claiming to be from someone you know but there is anything suspicious, check the actual email address being used by the contact. Foreign email addresses can masquerade as another email address. Before replying, check the actual email address being used, not just the contact name.

If they are bullying you to prove something, when you haven't initiated any matters or issues, do not disclose or provide any information. Ask them to prove their case and then check the veracity of the claim.

Mobile Phone Security

Always choose the highest level of security available on your mobile phone. Enable fingerprint identification if available; at the very least enable password sign-in. Consider a remote access backup so that if your phone is stolen you can remotely log in and disable the phone.

Privacy Laws

Australian privacy laws prevent businesses from releasing personal information and misusing it. Before you share any private or personal information, be certain of who it is you are giving the details to. Do not disclose your tax file number, bank account, passwords or other sensitive information.

Digital Signature

Authenticated digital signatures are allowable as an alternative to a hand-written signature. Not all electronic or digital signatures are authenticated - make sure the option you choose has a valid authentication process.

Employees

Educate staff on the importance of cyber security. Make sure all employees follow your standards and procedures. Make staff aware of internal policies you have regarding cyber and email security, internet use, downloads and so on.

You should have internal security procedures documented. For example, this may outline the process for double authorisation of all payments.

All staff should have individual logins and email addresses.

Consider installing computer monitoring software on employee computers.

When staff leave the business, remove access to all internal websites, accounting software, banks, supplier information and so on.